El Shorouk Academy
The Higher Institute of Engineering
Department of Communication and Electronics

Implementation of secured WiMAX based on FBGA

Supervised by:

DR. Mahmoud El shishtawy

Presented by:

1. Ahmed Magdy Kishk
2. ALY Tharwat Aly
3. Shimaa Ataa Abd el Zaher
4. Abd el rahman Monier Ragab
5. Neama Ahmed Aly
6. Sherif Ahmed Behary
7. Hossam Salah Hegazy
8. Sara Ahmed Helmy

Cairo 2010

All praise is for **ALLAH** for his gracious & grants upon us.

We wish to express our sincere gratitude to the person who stands besides us with his great competence, vision and direction to present our thoughts and visions in this book, to him we dedicate this book ...

To our teacher **Dr.Mahmoud El Shishtawy**.

We cannot forget to thank Head of Communication and Electronic Engineering Department

Prof.Dr. Dr.Mohammed El Morsy

for his contiguous encouragement for us to improve our skills and become innovators.

Abstract

A communication aid helps a person to communicate more effectively with those around them. Performance analysis and implementation of physical layer of wimax by using VHDL. This book is designed to give you how we can transmit and receive data in security sublayer and physical layer. Sufficient technical information has been included to instill a feeling for how systems are designed and operate. The book explanatory nature and broad coverage make it suitable as a textbook for university programs and internal training in communication systems design and planning. Nontechnical professionals in associated business management, contracts, legal and financial fields will find the book particularly helpful when they must deal with telecommunication projects and issues.

The book is organized into 7 chapters to get make an implementation to the physical layer of wimax to make a communication system. Chapter 1, "Overview of WiMAX", in this Chapter we discuss the meaning of wimax, its standers, the architecture of the wimax network, know the topologies of the system connection between the user and the base station, the advantages of WiMAX, disadvantages and its application.

Chapter 2, " Overview of OFDM" in this chapter know the meaning of Ofdm, the history of Ofdm, the advantages, disadvantages and the different between the OFDM, FDM, TDM and CDMA. And the main part in this chapter the Orthogonality, the meaning of Orthogonality, the multiplexing, Ofdm parameter, basics and real parameter.

Chapter 3,"Protocol Layers" in this chapter the frame structure of OFDM, channel coding, frame structure of MAC layer, bandwidth, quality of services, mobility management and power control. Chapter 4, "Physical layer ", in this chapter we study the block diagram of OFDM, the transfer the data in every block, the input out data and its mechanism. Chapter 5,"Encryption", in this chapter we study Attacks, Services, and Mechanisms, Security Attacks,_Passive and active Attacks,_DES Algorithm, Structure, Encryption, Decryption.

Chapter 6,"Implementaion of WiMAX of physical layer" in this chapter we use VHDL to make the implementation of WiMAX and show the input and the output data by using FPGA.

Chapter 7,"Conclusion and future work".

The book can be read sequentially from cover to cover because the material follows a consistent thread. All the elements and uses of spacecraft and earth stations are covered. Chapters also can be read out of sequence, if necessary, because each chapter explains the concepts relevant to it. References to other chapters are provided throughout. Once read, this book can be used as a reference because most of the terminology in current usage is defined and illustrated.

List of contents

Ch: 1. Overview of WiMAX: page

Ch: 2. Overview of OFDM:

List of contents

Ch: 3. Protocol layers:

Ch: 4. Physical layer WiMAX T_X & R_X:

List of contents

Ch: 6. Implementation of WiMAX PHY by VHDL:

List of contents

Ch: 7. Conclusions and suggestions of future work:

List of figures

Ch: 1. Overview of WiMAX: Page

List of figures

Ch: 2. Overview of OFDM:

List of figures

Ch: 3. Protocol layers:

Ch: 4. Physical layer WiMAX T_X &R_X:

Ch: 5. Security (Data Encryption Standard):

List of figures

Ch: 6. Implementation of WiMAX PHY by VHDL:

Ch: 7. Conclusions and suggestions of future work:

List of tables

Ch: 1. Overview of WiMAX: Page

Ch: 3. Protocol layers:

Ch: 4. Overview of WiMAX:

Ch: 5. Overview of WiMAX:

Abbreviation and Symbols

1xEV-DO 1x	Evolution data optimized
1xEV-DV 1x	Evolution data and voice
3DES	Triple data encryption standard
3G	Third generations
3GPP	Third-generation partnership project
3GPP2	Third generation partnership project-2
AAA	Authentication, authorization, and accounting
AAS	Advanced antenna systems
AC	Admission control
ACE	Active constellation extension
ADC	Analog-to-digital converter
ADSL	Asymmetric digital subscriber loop
AES	Advanced encryption standard
AF	Application function
AF	Assured forwarding
AK	Authentication key
AKA	Authentication and key agreement
AM	Amplitude modulation
AMC	Adaptive modulation and coding
AoA	Angle of arrival
AoD	Angle of departure
API	Application programming interface
AR	Access router
ARQ	Automatic repeat request
AS	Angular spread
ASN	Access services network
ASN-GW	ASN gateway
ASP	Application service provider
ATM	Asynchronous transfer mode
AWGN	Additive white Gaussian noise
AWS	Advanced wireless services
BE	Best effort
BEP	Bit error probability
BER	Bit error rate
BGCF	Breakout gateway control function
BLAST	Bell Labs layered spaced time
BLER	Block error rate
BPSK	Binary phase shift keying
BRS	Broadband radio services
BS	Base station
BSC	Base station controller
BSN	Block sequence number
BTS	Base station transceivers
CBC	Cipher-block chaining
CBR	Constant bit rate
CC	Convolution coding
CCDF	Complementary cumulative distribution function
CCI	Cochannel interference

Abbreviation and Symbols

CDF	Cumulative distribution function
CDMA	Code division multiple access
CGI	Common gateway interface
CHAP	Challenge handshake authentication protocol
CID	Connection identifier
CLT	Central limit theorem
CM	Cubic metric
CMAC	Cipher-based message authentication code
CMAC	Complexes multiply and accumulate
CN	Correspondent node
CoA	Care-of address
COPS	Common open policy service
CP	Cyclic prefix
CPE	Customer premise equipment
CPL	Call-processing language
CQICH	Channel-quality indicator channel
CRC	Cyclic redundancy check
CQI	Channel quality indicator
CS	Convergence sublayer
CSCF	Call session control function
CSI	Channel state information
CSMA	Carrier sense multiple access
CSN	Connectivity services network
CTC	Convolution turbo code
DAC	Digital-to-analog converter
DARS	Digital audio radio services
DC	Direct current
DCD	Downlink channel descriptor
DCF	Distributed coordination function
DECT	Digital-enhanced cordless telephony
DDFSE	Delayed-decision-feedback sequence estimation
DES	Data encryption standard
DFE	Decision-feedback equalizer
DFT	Discrete Fourier transform
DHCP	Dynamic host control protocol
DiffServ	Differentiated services
DL	Downlink
DNS	Domain name system
DoA	Direction of arrival
DOCSIS	Data over cable service interface specification
DP	Decision point
DPF	Data path function
DRM	Digital rights management
DS	Delay spread
DSA	Dynamic service allocation
DSC	Dynamic service change
DSCP	DiffServ code point
DSD	Dynamic service delete

Abbreviation and Symbols

DSL	Digital subscriber line
DSP	Digital-signal processing
DSTTD	Double space/time transmit diversity
DVB-H	Digital video broadcasting-handheld
EAP	Extensible authentication protocol
ECRM	Effective code rate map
EDGE	Enhanced data rate for GSM evolution
EESM	Exponentially effective SINR map
EF	Expedited forwarding
EGC	Equal gain combining
EIRP	Effective isotopic radiated power
EMSK	Enhanced master session key
EP	Enforcement point
ErtPS	Extended real-time packet service
ERT-VR	Extended real-time variable-rate service
ESP	Encapsulating security payload
ETH-CS	Ethernet convergence sublayer
ETRI	Electronics and Telecommunications Research Institute
ETSI	European Telecommunications Standards Institute
EVM	Error vector magnitude
FA	Foreign agent
FBSS	Fast base station switching
FCC	Federal Communications Commission
FCH	Frame control header
FDD	Frequency division duplexing
FDMA	Frequency division multiple access
FEC	Forward error correction
FEC	Forward equivalence class
FEQ	Frequency-domain equalization
FER	Frame error rate
FFT	fast Fourier transform
FHDC	frequency-hopping diversity code
FIB	forward information base
FIPS	Federal Information Processing Standard
FIR	finite impulse response
FM	frequency modulation
FSH	fragmentation subheader
FTP	file transfer protocol
FTTH	fiber-to-the-home
FUSC	full usage of subcarriers
FWA	fixed wireless access
GMH	generic MAC header
GPRS	GSM packet radio services
GRE	generic routing encapsulation
GSM	global system for mobile communications
GW	gateway
HA	home agent
HARQ	hybrid-ARQ

Abbreviation and Symbols

HDTV	high-definition television
HIPERMA	high-performance metropolitan area network
HHO	hard handover
HMAC	hash-based message authentication code
HO	handover
HoA	home address
HPA	high-power amplifier
HSDPA	high-speed downlink packet access
HSPA	high-speed packet access
HSS	home subscriber server
HSUPA	high-speed uplink packet access
HTTP	hypertext transfer protocol
HUMAN	high-speed unlicensed metropolitan area network
IBO	input backoff
ICI	intercarrier interference
ICMP	Internet control message protocol
I-CSCF	interrogating call session control function
IDFT	inverse discrete Fourier transform
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IFFT	inverse fast Fourier transform
IGMP	Internet group management protocol
IM	instant messaging
IMS	IP multimedia subsystem
IN	intelligent network
IntServ	integrated services
IP	Internet protocol
IP-CS	IP convergence sublayer
IPsec	IP security
IP-TV	Internet protocol television
IS	Integrated services
ISDN	Integrated services digital network
ISI	Inter-symbol interference
ITU	International Telecommunications Union
JAIN	Java for advanced intelligence network
KEK	Key encryption key
LAN	Local area network
LDAP	Lightweight directory access protocol
LDPC	Low-density parity codes
LDP-CR	Label distribution protocol/constraint-based routing
LER	Label-edge router
LLR	Log liklihood ratio
LMOS	Local multipoint distribution system
LMMSE	Linear minimum mean square error
LOS	Line of sight
LPF	Local policy function
LR	Location register

Abbreviation and Symbols

LS	Least squares
LSB	Least significant bit
LSP	Label switched path
LSR	Label switching router
LTE	Long-term evolution
MAC	Media access control
MAC	Message-authentication code
MAN	Metropolitan area network
MBS	Multicast broadcast service
MC-CDMA	Multicarrier CDMA
MCS	Modulation and coding scheme
MD5	Message-digest 5 algorithm
MDHO	Macro diversity handover
MIMO	Multiple input multiple outputs
MIC	Mean instantaneous capacity
MIP	Mobile IP
MIP-HA	Mobile IP home agent
MISO	Multiple input/single outputs
ML	Maximum likelihood
MLD	Maximum likelihood detection
MLSD	Maximum-likelihood sequence detection
MMDS	Multichannel multipoint distribution services
MMS	Multimedia messaging service
MMSE	Minimum mean square error
MN	Mobile node
MPDU	MAC protocol data unit
MPEG	Motion Picture Experts Group
MPLS	Multiprotocol label switching
M-QAM	Multilevel QAM
MRC	Maximal ratio combining
MRT	Maximum ratio transmission
MS	Mobile station
MSB	Most significant bit
MSDU	MAC service data unit
MSE	Mean square error
MSK	Master session key
MSL	Minimum signal level
MSR	Maximum sum rate
MUD	Multiuser detection
NAI	Network access identifier
NAP	Network access provider
NAS	Network access server
NAT	Network address translation
NLOS	Non–line-of-sight
NRM	Network reference model
nrtPS	Non–real n time polling service
NSP	Network services provider
NTP	Network timing protocol

Abbreviation and Symbols

NWG	Network Working Group
OBO	Output backoff
OC	Optimum combiner
OCI	Other-cell interference
OFDM	Orthogonal frequency division multiplexing
OFDMA	Orthogonal frequency division multiple access
OSA	Open systems architecture
OSI	Open systems interconnect
O-SIC	Ordered successive cancellation
OSS	Operational support systems
OSTBC	Orthogonal space/time block code
PA	Paging agent
PAP	Password authentication protocol
PAPR	Peak-to-average-power ratio
PAR	Peak-to-average ratio
PC	Paging controller
PCS	Personal communications services
P-CSCF	Proxy call session control function
PDA	Personal data assistant
PDF	Probability density function
PDP	Policy decision point
PDU	Packet data unit
PEAP	Protected extensible authentication protocol
PEP	Policy enforcement point
PER	Packet error rate
PF	Proportional fairness; policy function
PG	Paging group
PHB	Per hop behavior
PHS	Packet header suppression
PHSF	PHS field
PHSI	PHS index
PHSM	PHS mask
PHSV	PHS verify
PKI	Public key infrastructure
PKM	Privacy and key management
PM	Phase modulation
PMIP	Proxy mobile IP
PMK	Pair wise master key
PN	Pseudo noise
PoA	Point of attachment
PPP	Point-to-point protocol
PR	Policy rule
PRC	Proportional rate constraints
P/S	Parallel to serial
PSH	Packing subheader
PSK	preshared key
PSTN	Public switched telephone network
PTS	Partial transmit sequence

Abbreviation and Symbols

PUSC	Partial usage of subcarriers
QoS	Quality of service
QAM	quadrature amplitude modulation
QPSK	quadrature phase shift keying
RADIUS	Remote access dial-in user service
RF	Radio frequency
RFC	Request for comments
RMS	Root mean square
ROHC	Robust header compression
RP	Reference point
RR	Radio resource
RR	Round-robin
RRA	Radio resource agent
RRC	Radio resource controller
RRM	Radio resource management
RS	Reed Solomon
RSA	Rivest-Shamir-Adleman
RSS	Received signal strength
RSSE	Reduced-state sequence estimation
RSSI	Received signal strength indicator
RSVP	Resource reservation protocol
RTCP	Real-time control protocol
RTP	Real-time transport protocol
rtPS	Real-time polling service
RTT	Roundtrip time
RUIM	Removable user identity module
SA	Security association
SC	Selection combining
S-CSCF	Serving call session control function
SCTP	Stream control transport protocol
SDP	Session description protocol
SDU	Service data unit
SET	Secure electronic transactions
SF	Service flow; shadow fading
SFA	Service flow authorization
SFBC	Space/frequency block code
SFID	Service flow identifier
SFM	Service flow management
SGSN	Serving GPRS support node
SH	Sub header
SHA	Secure hash algorithm
SIC	Successive interference cancellation
SII	System identity information
SIM	Subscriber identity module
SIMO	Single input/multiple output
SINR	Signal-to-interference-plus-noise ratio
SIP	Session initiation protocol
SIR	Signal-to-interference ratio

Abbreviation and Symbols

SISO	Single input/single output
SLA	Service-level agreement
SLM	Selected mapping
SM	Spatial multiplexing
SME	Small and medium enterprise
SMS	Short messaging service
SNDR	Signal-to-noise and distortion ratio
SNR	Signal-to-noise ratio
SOFDMA	Sealable OFDMA
SOHO	Small office/home office
SOVA	Soft input/soft output
S/P	Serial to parallel
SPI	Security parameter index
SPID	Sub packet identity
SPM	Spatial-channel model
SPWG	Service Provider Working Group
SS	Subscriber station
SSL	Secure sockets layer
STBC	Space/time block code
SUI	Standford University Interim
SVD	Singular-value decomposition
TCP	Transport control protocol
TD-SCDMA	Time division/synchronous CDMA
TDD	Time division duplexing
TDL	Tap-delay line
TDM	Time division multiplexing
TDMA	Time division multiple access
TE	Traffic engineering
TEK	Traffic encryption key
TLS	Transport-layer security
TOS	Type of service
TR	Tone reservation
TSD	Transmit selection diversity
TTLS	Tunneled transport layer security
TUSC	Tile usage of subcarriers
UA	User agent
UCD	Uplink channel descriptor
UDP	User datagram protocol
UGS	Unsolicited grant services
UHF	Ultrahigh frequency
UICC	Universal integrated circuit card
UL	Uplink
ULA	Uniform linear array
UMTS	Universal mobile telephone system
U-NII	Unlicensed national information infrastructure
URL	Universal resource locator
USIM	Universal subscriber identity module
VDSL	Very high data rate digital subscriber loop

Overview of WiMAX

Chapter 1

1.1 Introduction

The experienced growth in the use of digital networks has led to the need for the design of new communication networks with higher capacity. The telecommunication industry is also changing, with a demand for a greater range of services, such as video conferences, or applications with multimedia contents. The increased reliance on computer networking and the Internet has resulted in a wider demand for connectivity to be provided "any where, any time", leading to a rise in the requirements for higher capacity and high reliability broadband wireless telecommunication systems.

Broadband availability brings high performance connectivity to over a billion users' worldwide, thus developing new wireless broadband standards and technologies that will rapidly span wireless coverage. Wireless digital communications are an emerging field that has experienced an spectacular expansion during the last several years. Moreover, the huge uptake rate of mobile phone technology, WLAN (Wireless Local Area Network) and the exponential growth of Internet have resulted in an increased demand for new methods of obtaining high capacity wireless networks.

Worldwide Interoperability for Microwave Access, known as WiMAX, is a wireless networking standard which aims for addressing interoperability across IEEE802.16 standard-based products. WiMAX defines a *WMAN,* a kind of a huge hot-spot that provides interoperable broadband wireless connectivity to fixed, portable, and nomadic users. It allows communications which have no direct visibility, coming up as an alternative connection for cable, DSL and T1/E1 systems, as well as a possible transport network for Wi-Fi hot-spots, thus becoming a solution to develop broadband industry platforms. Likewise, products based on WiMAX technology can be combined with other technologies to offer broadband access in many of the possible scenarios of

utilization, as shown in ***Figure 1.1***, where examples of the deployment of WiMAX systems are illustrated.

WiMAX will substitute other broadband technologies competing in the same segment and will become an excellent solution for the deployment of the well-known last mile infrastructures in places where it is very difficult to get with other technologies, such as cable or DSL, and where the costs of deployment and maintenance of such technologies would not be profitable. In this way, WiMAX will connect rural areas in developing countries as well as underserved metropolitan areas. It can even be used to deliver backhaul for carrier structures, enterprise campus, and Wi-Fi hot-spots. WiMAX offers a good solution for these challenges because it provides a cost-effective, rapidly deployable solution.

Additionally, WiMAX will represent a serious competitor to 3G (Third Generation) cellular systems as high speed mobile data applications will be achieved with the 802.16e specification.

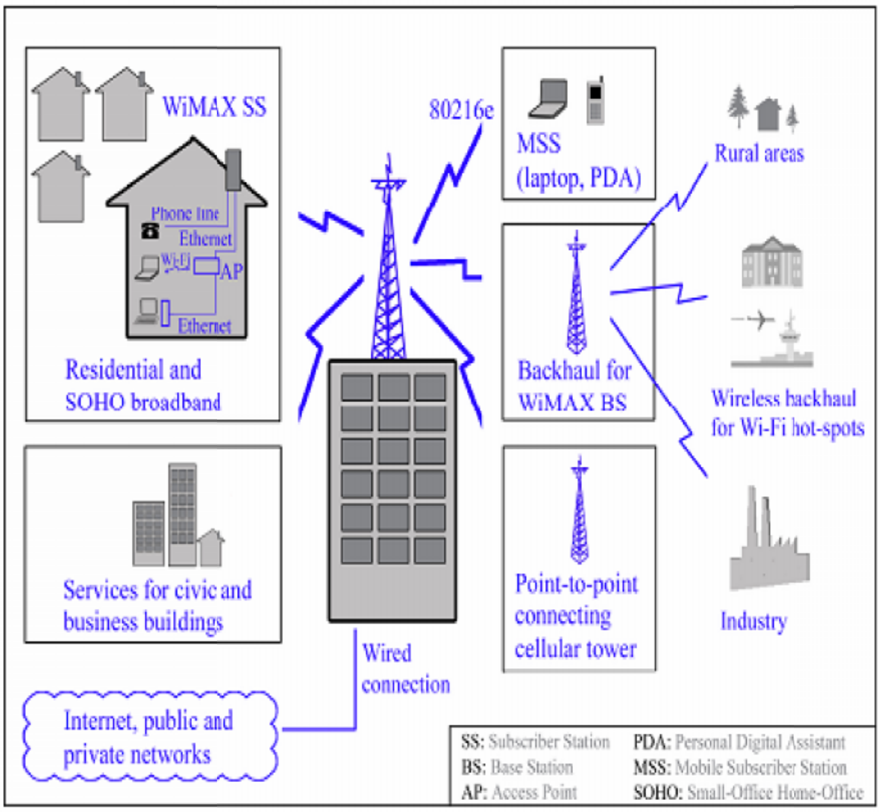


***Fig.1.1:** Possible scenarios for the deployment of WiMAX*

1.2 What is WiMAX?

WiMAX is stand for (*Worldwide Interoperability for Microwave Access*) is an emerging technology that is designed to deliver fixed, and more recently, mobile broadband connectivity. The WiMAX trade name is used to group a number of wireless technologies that have emerged from the IEEE (*Institute of Electrical and Electronics Engineers*) 802.16 Wireless MAN (*Metropolitan Area Network*) standards. The main two standards are identified as 802.16-2004 (*October 2004)* and802.16e (*December 2005*), with 802.16e introducing mobility and currently receiving a great deal of interest in the telecoms world.

1.2.1 The WiMAX standard

The IEEE 802.16 standard was firstly designed to address communications with direct visibility in the frequency band from 10 to 66 GHz. Due to the fact that non-line-of-sight transmissions are difficult when communicating at high frequencies, the amendment 802.16a was specified for working in a lower frequency band, between 2 and 11 GHz. The IEEE 802.16d specification is a variation of the fixed standard (IEEE 802.16a) with the main advantage of optimizing the power consumption of the mobile devices. The last revision of this specification is better known as IEEE 802.16-2004.

On the other hand, the IEEE 802.16e standard is an amendment to the 802.16-2004 base specification with the aim of targeting the mobile market by adding portability.

WiMAX standard-based products are designed to work not only with IEEE 802.16-2004 but also with the IEEE 802.16e specification. While the 802.16-2004 is primarily intended for stationary transmission, the 802.16e is oriented to both stationary and mobile deployments.

1.2.2 Background on IEEE 802.16 and WiMAX

The IEEE 802.16 group was formed in 1998 to develop an air-interface standard for wireless broadband. The group's initial focus was the development of a LOS-based point-to-multipoint wireless broadband system for operation in the *10GHz–66GHz* millimeter wave band. The resulting standard the original 802.16 standard, completed in December 2001 was based on a single-carrier physical (PHY) layer with a burst time division multiplexed (TDM) MAC layer. Many of the concepts related to the MAC layer were adapted for wireless from the popular cable modem DOCSIS (data over cable service interface specification) standard.

The IEEE 802.16 group subsequently produced 802.16a, an amendment to the standard, to include NLOS applications in the 2GHz–11GHz band, using an *orthogonal frequency division multiplexing* (OFDM)-based physical layer. Additions to the MAC layer, such as support for *orthogonal frequency division multiple access* (OFDMA), were also included. Further revisions resulted in a new standard in 2004, called IEEE 802.16-2004, which replaced all prior versions and formed the basis for the first WiMAX solution. These early WiMAX solutions based on IEEE 802.16-2004 targeted fixed applications, and we will refer to these as fixed WiMAX. In December 2005, the IEEE group completed and approved IFEEE 802.16e-2005, an amendment to the IEEE 802.16-2004 standard that added mobility support. The IEEE 802.16e-2005 forms the basis for the WiMAX solution for nomadic and mobile applications and is often referred to as mobile WiMAX.

The basic characteristics of the various IEEE 802.16 standards are summarized in ***Table1.1.***

Table 1.1: *Basic Data on IEEE 802.16 Standards*

	802.16	802.16-2004	802.16e-2005
Status	Completed December 2001	Completed June 2004	Completed December 2005
Frequency band	10GHz–66GHz	2GHz–11GHz	2GHz–11GHz for fixed; 2GHz–6GHz for mobile applications
Application	Fixed LOS	Fixed NLOS	Fixed and mobile NLOS
MAC architecture	Point-to-multipoint, mesh	Point-to-multipoint, mesh	Point-to-multipoint, mesh
Transmission scheme	Single carrier only	Single carrier, 256 OFDM or 2,048 OFDM	Single carrier, 256 OFDM or scalable OFDM with 128, 512, 1,024, or 2,048 subcarriers
Modulation	QPSK, 16 QAM, 64 QAM	QPSK, 16 QAM, 64 QAM	QPSK, 16 QAM, 64 QAM
Gross data rate	32Mbps–134.4Mbps	1Mbps–75Mbps	1Mbps–75Mbps
Multiplexing	Burst TDM/TDMA	Burst TDM/TDMA/OFDMA	Burst TDM/TDMA/OFDMA
Duplexing	TDD and FDD	TDD and FDD	TDD and FDD
Channel bandwidths	20MHz, 25MHz, 28MHz	1.75MHz, 3.5MHz, 7MHz, 14MHz, 1.25MHz, 5MHz, 10MHz, 15MHz, 8.75MHz	1.75MHz, 3.5MHz, 7MHz, 14MHz, 1.25MHz, 5MHz, 10MHz, 15MHz, 8.75MHz
Air-interface designation	WirelessMAN-SC	WirelessMAN-SCa WirelessMAN-OFDM WirelessMAN-OFDMA WirelessHUMAN[a]	WirelessMAN-SCa WirelessMAN-OFDM WirelessMAN-OFDMA WirelessHUMAN[a]
WiMAX implementation	None	256 - OFDM as Fixed WiMAX	Scalable OFDMA as Mobile WiMAX

a. WirelessHUMAN (wireless high-speed unlicensed MAN) is similar to OFDM-PHY (physical layer) but mandates dynamic frequency selection for license-exempt bands.

1.3 WiMAX Spectrum Availability

WiMAX 802.16-2004 and 802.16e operate at frequencies below 11GHz and 6GHz respectively. So far the most viable spectrum is available at the unlicensed 2.4GHz and 5.8GHz bands, as well as the 2.3GHz, 2.5GHz and 3.5GHz licensed bands. In addition, it may be possible to use the700MHz analogue TV band (once released). With all these possible frequencies, the main issue is now one of worldwide interoperability and the fact that WiMAX devices may have to support multiple frequency bands to be globally compatible.

1.3.1 licensed

The main issue with licensed spectrum is that it usually comes at a high price. It is however vital for operators carriers wanting to offer a high level quality service, ensuring exclusive use of the spectrum and thus protecting the users from unwanted interference.

- 700MHz Band - This band is currently utilized worldwide for analogue television broadcasters.
- 2.3GHz Band - In Australia, New Zealand and the United States, this band is currently utilized for other systems, such that the spectrum is not that attractive. It is also used in South Korea where it is used for WiBRO (Wireless Broadband), an early adoption of a WiMAX 802.16e standard.
- 2.5GHz Band - This band is gaining a lot of attention since it is available for use in North America and Latin America. It is also soon to be available across Europe, once the 3G (Third Generation) extension bands are auctioned off. This may cause issues since the band could be bought by 3G operator's carrier wanting to improve their offering.
- 3.5GHz Band - This band is currently available for use in most countries with the exception of the United States. In many countries this band also has various regulator license restrictions, which in some cases limit the use of mobility.

1.3.2 Unlicensed

It is worth noting that the 2.4GHz and 5.8GHz are unlicensed bands and are currently being utilized by such technologies as Wi-Fi and Bluetooth. The term unlicensed spectrum implies that there is no regulation governing its use.

However in Europe a concept of "light licensed" spectrum applies. In this scenario, the users have to indicate their intent to use this spectrum. The idea behind this is to enable regulators to identify usage and potentially control the number of licensees, thus minimizing unwanted loading and interference.

1.4 WiMAX Network Architecture& Network Reference Model(NRM)

The IEEE 802.16-2004 standard provides the air interface for WiMAX but does not define the full end-to-end WiMAX network. The WiMAX Forum's Network Working Group, is responsible for developing the end-to-end network requirements, architecture, and protocols for WiMAX, using IEEE 802.16e-2005 as the air interface.

The WiMAX NWG has developed a network reference model to serve as an architecture framework for WiMAX deployments and to ensure interoperability among various WiMAX equipment and operators.

The network reference model envisions unified network architecture for supporting fixed, nomadic, and mobile deployments and is based on an IP service model. ***Figure 1.2*** shows a simplified illustration of IP-based WiMAX network architecture.

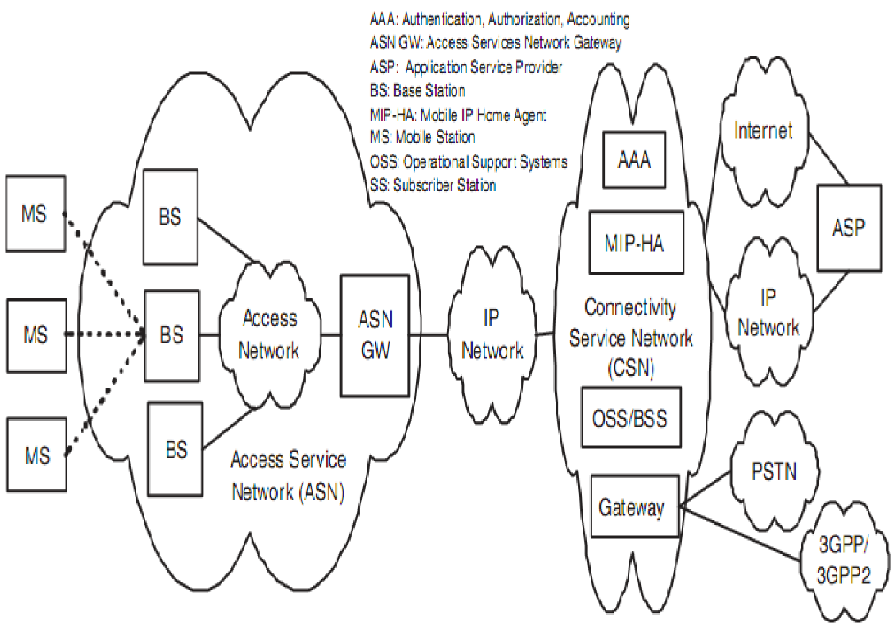


Fig.1.2: WiMAX Network Architecture

The overall network may be logically divided into three parts:

1) ***Mobile Stations*****:** used by the end user to access the network.

2) **The Access Service Network (ASN):** which comprises one or more base stations and one or more ASN gateways that form the radio access network at the edge.

3) **The Connectivity Service Network (CSN):** which provides IP connectivity and all the IP core network functions.

The architecture framework is defined such that the multiple players can be part of the WiMAX service value chain.

More specifically, the architecture allows for three separate business entities:

1) **Network Access Provider (NAP):** which owns and operates the ASN.

2) **Network Services Provider (NSP):** which provides IP connectivity and WiMAX services to subscribers using the ASN infrastructure provided by one or more NAPs.

3) **Application Service Provider (ASP):** which can provide value-added services such as multimedia applications using IMS (IP multimedia subsystem) and corporate VPN (virtual private networks) that run on top of IP.

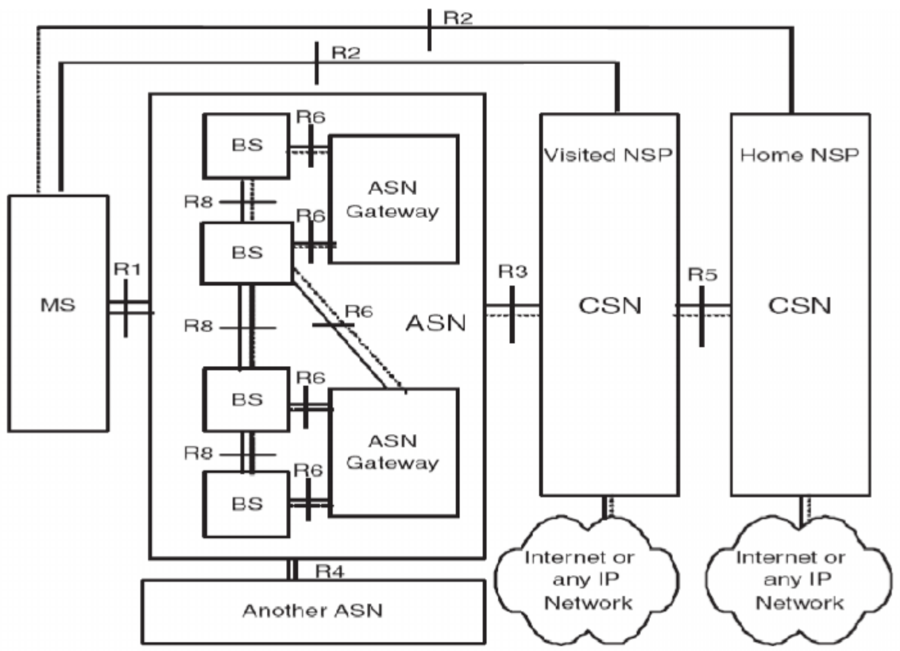


Fig.1.3: WiMAX Network reference model

This separation between NAP, NSP, and ASP is designed to enable a richer ecosystem for WiMAX service business, leading to more competition and hence better services.

The network reference model (NRM) developed by the WiMAX Forum NWG defines a number of functional entities and interfaces between those entities. (The interfaces are referred to as reference points.) ***Figure 1.3*** shows some of the more important functional entities.

Base station (BS): The BS is responsible for providing the air interface to the MS. Additional functions that may be part of the BS are micro mobility management functions, such as handoff triggering and tunnel establishment, radio resource management, QOS policy enforcement, traffic classification, DHCP (Dynamic Host Control Protocol) proxy, key management, session management, and multicast group management.

Access service network gateway (ASN-GW): The ASN gateway typically acts as a layer 2 traffic aggregation points within an ASN. Additional functions that may be part of the ASN gateway include intra-ASN location management and paging, radio resource management and admission control, caching of subscriber profiles and encryption keys, AAA client functionality, establishment and management of mobility tunnel with base stations, QOS and policy enforcement, and foreign agent functionality for mobile IP, and routing to the selected CSN.

Connectivity service network (CSN): The CSN provides connectivity to the Internet, ASP, other public networks, and corporate networks. The CSN is owned by the NSP and includes servers that support authentication for the devices, users, and specific services. The CSN also provides per user policy management of QOS and security. The CSN is also responsible for IP address management, support for roaming between different NSPs, location management between ASNs, and mobility and roaming between ASNs. Further, CSN can also provide gateways and interworking with other networks, such as PSTN (public switched telephone network), 3GPP, and 3GPP2.

The WiMAX architecture framework allows for the flexible decomposition and/or combination of functional entities when building the physical entities.

For example, the ASN may be decomposed into base station transceivers (BST), base station controllers (BSC), and an ASNGW analogous to the GSM model of BTS, BSC, and Serving GPRS Support Node (SGSN).
It is also possible to collapse the BS and ASN-GW into a single unit, which could be thought of as a WiMAX router. Such a design is often referred to as a distributed, or flat, architecture. By not mandating a single physical ASN or CSN topology, the reference architecture allows for vendor/ operator differentiation.

In addition to functional entities, the reference architecture defines interfaces, called reference points, between function entities. The interfaces carry control and management protocols— mostly IETF-developed network and transport-layer protocols—in support of several functions, such as mobility, security, and QOS, in addition to bearer data. **Figure 1.4**shows an example.

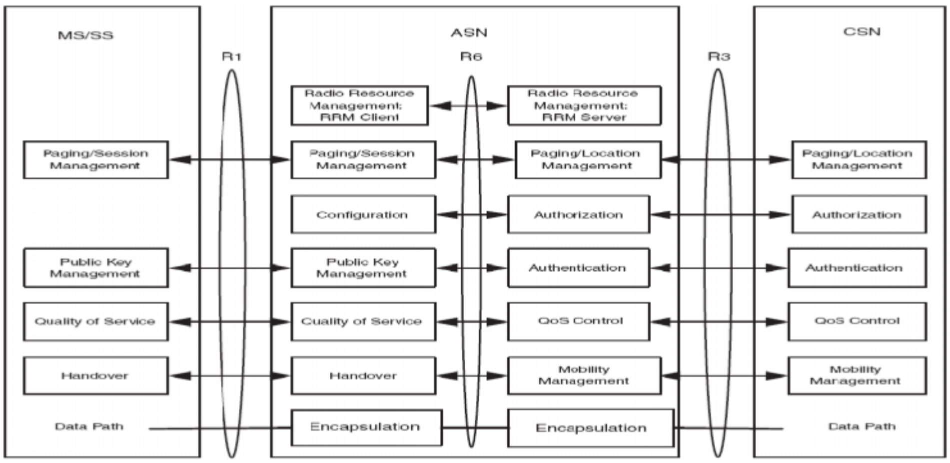


Fig.1.4: Functions performed across reference points

The WiMAX network reference model defines reference points between:

1) ***MS and the ASN:*** called R1, which in addition to the air interface includes protocols in the management plane.

2) ***MS and CSN:*** called R2, which provides authentication, service authorization, IP configuration, and mobility management.

3) ***ASN and CSN:*** called R3, to support policy enforcement and mobility management.
4) ***ASN and ASN:*** called R4, to support inter-ASN mobility.

5) ***CSN and CSN:*** called R5, to support roaming across multiple NSPs.

6) ***BS and ASN-GW***

7) ***BS to BS:*** called R7, to facilitate fast, seamless handover.

1.5 WIMAX Topologies

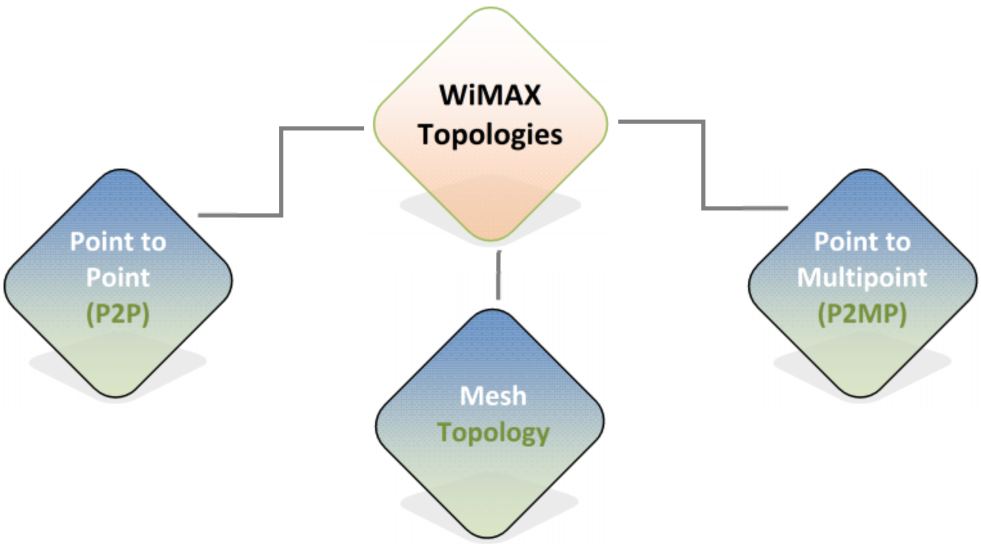


Fig.1.5: *WiMAX Various Topologies*

1.5.1 Point-to-point (P2P)

Point to point is used where there are two points of interest: one sender and one receiver. This is also a scenario for backhaul or the transport from the data source (data center, co-Lo facility, fiber POP, Central Office, etc.) to the subscriber or for a point for distribution using point to multipoint architecture. Backhaul radios comprise an industry of their own within the wireless industry. As the architecture calls for a highly focused beam between two points range and throughput of point-to point radios will be higher than that of point-to-multipoint products, as shown in ***Figure1.6***.

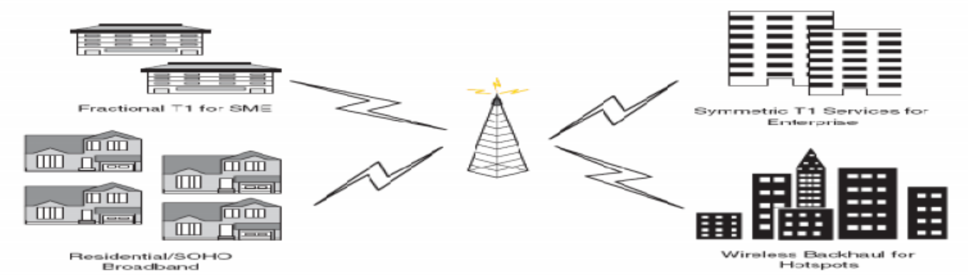


Fig.1.6: *Point-to-point WiMAX Configurations*

1.5.2 Point-to-Multipoint (PMP)

Point-to-multipoint is synonymous with distribution. One base station can service hundreds of dissimilar subscribers in terms of bandwidth and services, as shown in ***Figure 1.7***.

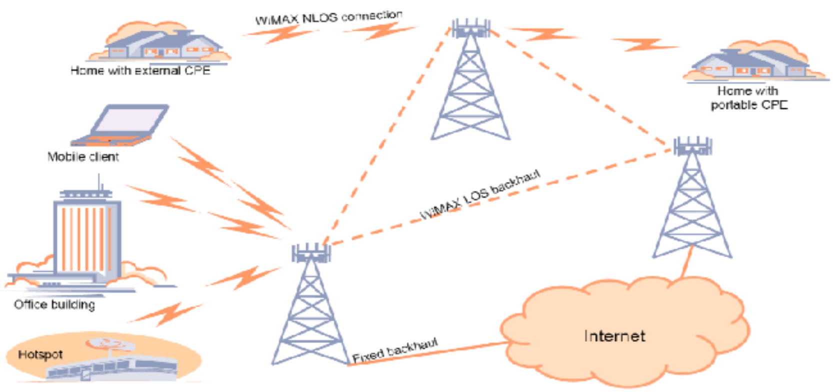


Fig.1.7: *Point-to-Multipoint WiMAX Configurations*

1.5.3 Mesh Topology

Mesh topology is not supported by existing IEEE's wireless LAN standards but it becomes popular as city-wide (municipal) Wi-Fi network deployment gains more supporters day after day. In a mesh network, each node (i.e. base station or access point) connects to several neighboring nodes and on to a mesh gateway (i.e. a base station that aggregates the mesh network traffic and routes it to the Internet). Since each node has many routes to a mesh gateway, mesh network is very reliable. But mesh network is more complex to manage and poses interference challenge especially for operation in a license-exempt band such as in Wi-Fi case. As shown in ***Figure 1.8***.

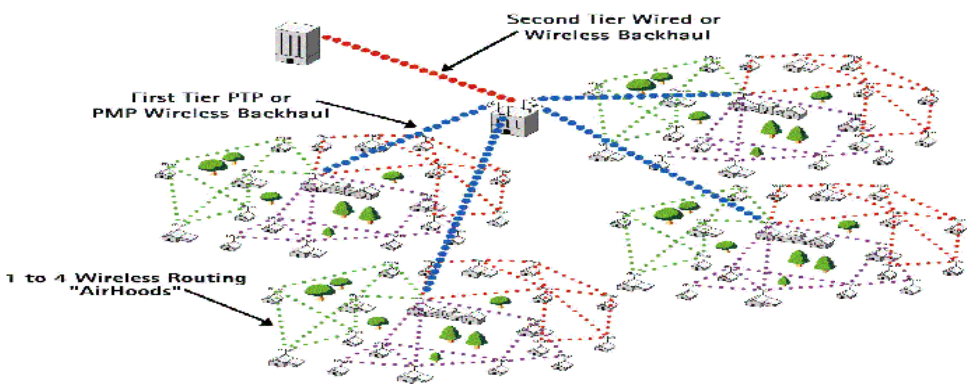
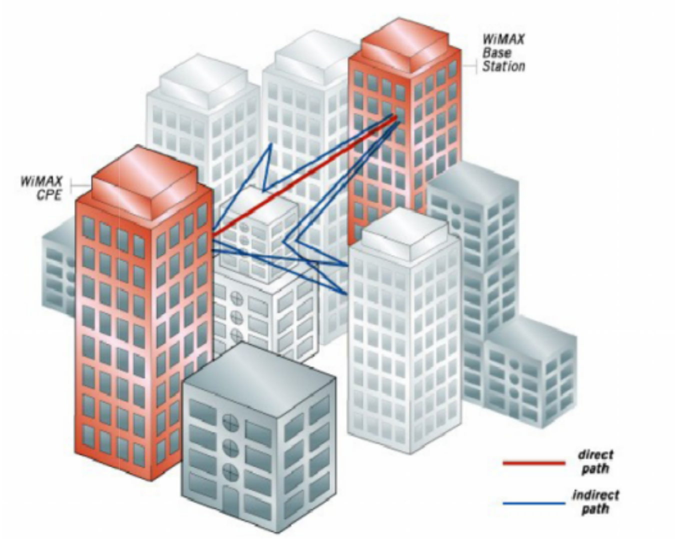


Fig.1.8: Mesh Network with Wi-Fi and/or WiMAX

1.6 Line of sight (LOS) & Non-line of sight (NLOS)

Earlier wireless technologies (LMDS, MMDS for example) were unsuccessful in the mass market as they could not deliver services in non-line-of-sight scenarios. This limited the number of subscribers they could reach and, given the high cost of base stations and CPE, those business plans failed. WiMAX functions best in line of sight situations and, unlike those earlier technologies, offers acceptable range and throughput to subscribers who are not line of sight to the base station. Buildings between the base station and the subscriber diminish the range and throughput, but in an urban environment, the signal will still be strong enough to deliver adequate service. Given WiMAX's ability to deliver services non-line-of-sight, the WiMAX service provider can reach many customers in high-rise office buildings to achieve a low cost per subscriber because so many subscribers can be reached from one base station.



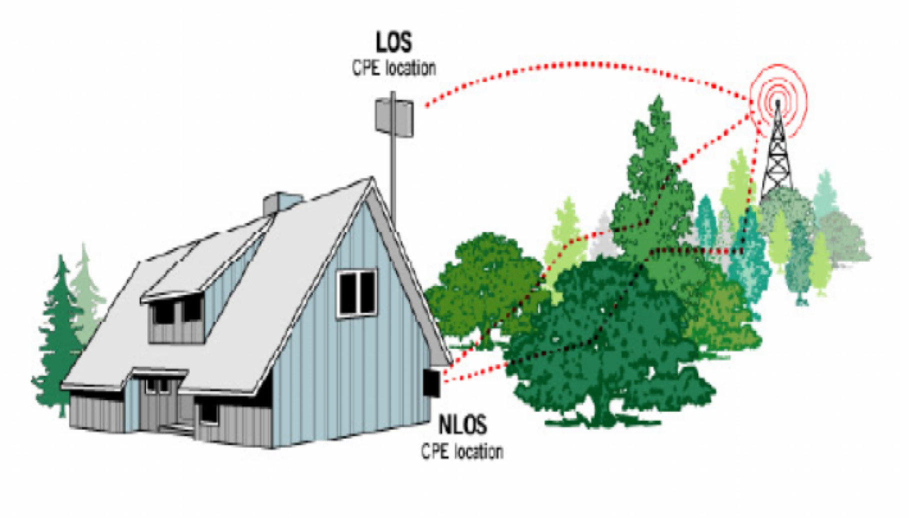


Fig.1.9& 1.10: The difference between line of sight and non-line of sight

1.7 WiMAX Antennas

WiMAX antennas, just like the antennas for car radio, cell phone, FM radio, or TV, are designed to optimize performance for a given application. The figure above illustrates the three main types of antennas used in WiMAX deployments. From top to bottom is an Omni directional, sector and panel antenna each has a specific function. As shown in ***Figure 1.11*** .

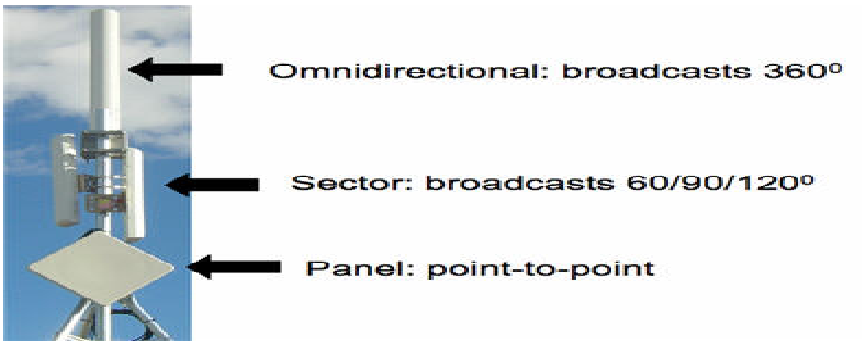


Fig.1.11: Different antenna types are designed for different applications

1.7.1 Omni directional antenna

Omni directional antennas are used for point-to-multipoint configurations. The main drawback to an Omni directional antenna is that its energy is greatly diffused in broadcasting 360 degrees. This limits its range and ultimately signals strength. Omni directional antennas are good for situations where there are a lot of subscribers located very close to the base station. An example of

Omni directional application is a Wi-Fi hotspot where the range is less than 100 meters and subscribers are concentrated in a small area. As shown in ***Figure 1.12***.

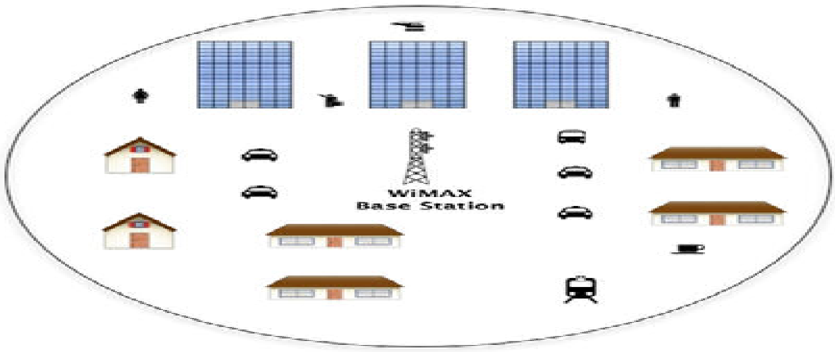


Fig.1.12: *An Omni-directional antenna broadcasts 360 degrees from the base station*

1.7.2 Sector antennas

A sector antenna, by focusing the beam in a more focused area, offers greater range and throughput with less energy. Many operators will use sector antennas to cover a 360-degree service area rather than use an Omni directional antenna due to the superior performance of sector antennas over an Omni directional antenna. As shown in ***Figure 1.13***.

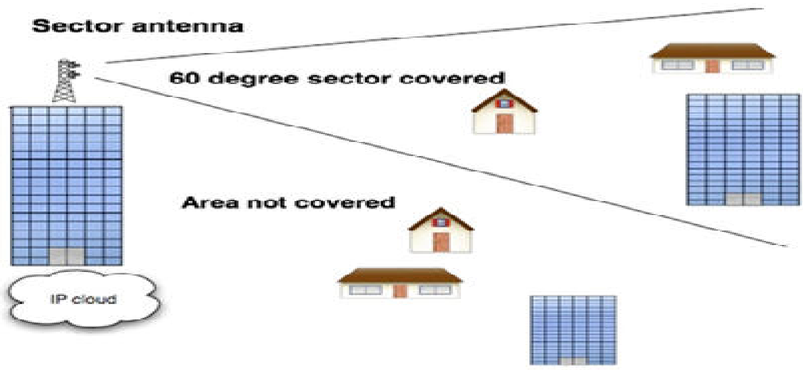


Fig.1.13: Sector antennas are focused on smaller sectors

1.7.3 Panel antennas

Panel antennas are usually a flat panel of about one foot square. They can also be a configuration where potentially the WiMAX radio is contained in the square antenna enclosure. Such configurations are powered via the Ethernet cable that connects the radio/antenna combination to the wider network. That

power source is known as Power over Ethernet (POE). This streamlines deployments, as there is no need to house the radio in a separate, weatherproof enclosure if outdoors or in a wiring closet if indoors. This configuration can also be very handy for relays. As shown in ***Figure 1.14***.

Fig.1.14: *Panel antennas are most often used for point to-point applications*

A WiMAX system consists of two parts:

- ***A WiMAX tower*****:** similar in concept to a cell phone tower a single WiMAX tower can provide coverage to a very large area ~~as~~ big as 3,000 square miles (8,000 square km.)
- ***A WiMAX receiver*****:** The receiver and antenna could be a small box or PCMCIA card, or they could be built into a laptop the way Wi-Fi access is today.

1.8 Subscriber Stations

The technical term for customer premise equipment (CPE) is subscriber station. The generally accepted marketing terms now focus on either "indoor CPE" or "outdoor CPE". There are advantages and disadvantages to both deployment schemes as described below.

1.8.1 Outdoor CPE

An outdoor CPE device, Note mounting brackets for outdoor mounting on roof or side of building. Outdoor CPEs are very simply put, offers somewhat better performance over indoor CPE given that walls of concrete or brick, RF blocking glass or steel in the building's walls, do not impede WiMAX reception. In many cases the subscriber may wish to utilize an outdoor CPE in order to maximize reception via a line of sight connection to the base station

not possible with indoor CPE. Outdoor CPE will cost more than indoor CPE due to a number of factors including extra measures necessary to make outdoor CPE weather resistant.

Fig.1.15: *An Outdoor WiMAX CPE device*

1.8.2 Indoor CPE

The most significant advantage of indoor over outdoor CPE is that it is installed by the subscriber. This frees the service provider from the expense of "truck roll" or installation. In addition, it can be sold online or in a retail facility thus sparing the service provider a trip to the customer site. Indoor CPE also allows a certain instant gratification for the subscriber in that there is no wait time for installation by the service provider. Currently, many telephone companies require a one month wait between placement of order and in stallation of T1 or E1 services. In addition, an instant delivery of service is very appealing to the business subscriber in the event of a network outage by the incumbent service provider.

Fig.1.16: *Indoor WiMAX CPE with telephone handset and VoIP adapter*

1.9 Relationship with other wireless technologies

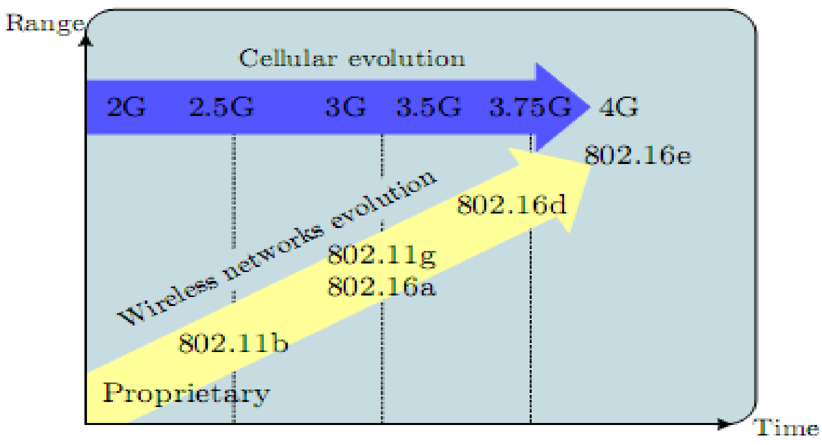


Fig.1.17: *Convergence in wireless communications*

Wireless access to data networks is expected to be an area of rapid growth for mobile communication systems. The huge uptake rate of mobile phone technologies, WLANs and the exponential growth that is experiencing the use of the Internet have resulted in an increased demand for new methods to obtain high capacity wireless networks. WiMAX may be seen as the fourth generation (4G) of mobile systems as the convergence of cellular telephony, computing, Internet access, and potentially many multimedia applications become a real fact. The mentioned convergence between wireless and cellular networks is illustrated in ***Figure 1.17.***

In any case, both WLAN and cellular mobile applications are being widely expanded to offer the demanded wireless access. However, they experience several difficulties for reaching a complete mobile broadband access, bounded by factors such as bandwidth, coverage area, and infrastructure costs. On one hand, Wi-Fi provides a high data rate, but only on a short range of distances and with a slow movement of the user.

On the other hand, UMTS offers larger ranges and vehicular mobility, but instead, it provides lower data rates, and requires high investments for its deployment. WiMAX tries to balance this situation . As shown in ***Figure 1.18***, it fills the gap between Wi-Fi and UMTS, thus providing vehicular mobility (included in IEEE 802.16e), and high service areas and data rates.

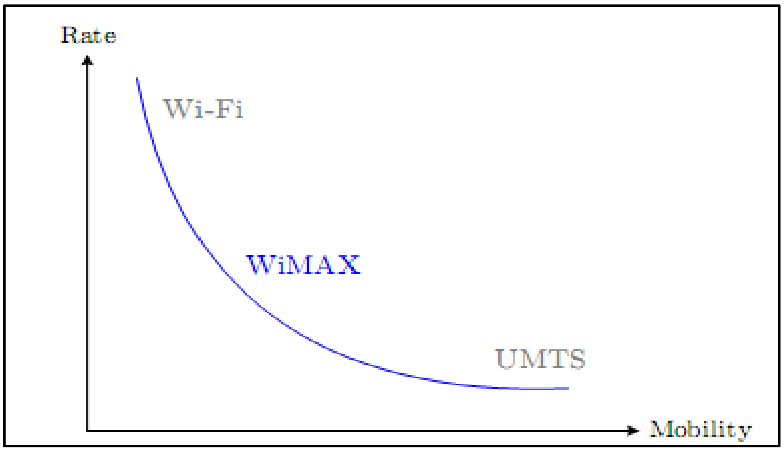


Fig.1.18: WiMAX fills the gap between Wi-Fi and UMTS

Therefore, while WiMAX will complement Wi-Fi and UMTS in some of the possible scenarios where these systems are not sufficiently developed, i.e. they face several problems in the deployment and they do not offer enough capacity to serve all possible users, WiMAX will compete with Wi-Fi and UMTS also in other possible scenarios, where, in general, the costs in the deployment, maintenance, or just the supply of the service would not be profitable. ***Table 1.3*** gives an overview on the comparison between the mentioned systems, WiMAX and its two closest competitors, Wi-Fi and UMTS. A deeper analysis of these three systems will be developed next.

Table 1.2: Comparative table between Wi-Fi, WiMAX and UMTS

	Wi-Fi	WiMAX		UMTS HSDPA
Standard	IEEE 802.11	IEEE 802.16		IMT2000[14]
Channel width	Fixed 20 MHz	Variable $\leq$ 20 MHz	Variable $\leq$ 28 MHz	Fixed 5 MHz
Spectrum	2.4/5.2 GHz	2-11 GHz	10-66 GHz	~2 GHz
Data rate	2/54 Mbps	70 Mbps	240 Mbps	1/14 Mbps
Range	100 m	1-7 km	12-15 km	50 km
Multiplexing	TDM	FDM/TDM	FDM/TDM	FDM
Transmission	SS[15]/OFDM	OFDM/OFDMA	SC	WCDMA
Mobility	Pedestrian	Vehicular (802.16e)	No	Vehicular
Advantages	Throughput and costs	Throughput and range		Mobility and range
Disadvantages	Short range	Interference issues?		Low rates and expensive

1.9.1 WiMAX vs. Wi-Fi

Wi-Fi or WLAN is the name with which the IEEE 802.11 standard-based products are known. It includes the 802.11a specification, capable to offer data rates of 54 Mbps working in the frequency band of 5.2 GHz; and the 802.11b specification, in the 2.4 GHz frequency band, which provides users with data rates of 11 Mbps. This technology has generally a coverage area of 100 meters and fixed channel bandwidths of 20MHz.

WiMAX appeared to fulfil the need for delivering wireless access to MANs. It was designed to offer BWA services to metropolitan areas providing users with larger coverage ranges and higher data rates. WiMAX systems are able to support users in ranges up to 50 km with a direct visibility to the base station and ranges from 1 to 7 km where no visibility is available. Rates from 70 to 240 Mbps are offered and can be achieved with this technology.

However, WiMAX does not create a conflict with the mentioned Wi-Fi, as they are complementary technologies. WiMAX provides a low cost way to backhaul Wi-Fi hot-spots and WLAN points in businesses and homes, offering a wireless last mile extension for cable and DSL infrastructures.

1.9.2 WiMAX vs. UMTS

UMTS is identified with the so-called third generation of cellular networks Standardized by the 3GPP.The frequency bands that are assigned to this technology are the licensed frequencies from 1885 to 2025 MHz, and from 2110 to 2200MHz. It uses wideband code division multiple access (WCDMA) as the carrier modulation scheme, and it has been specified as an integrated solution for mobile voice and data with wide coverage area, offering data rates that may decrease while the velocity of the user increases. This system provides for theoretical bit rates of up to 384 kbps in high mobility situations, which rise as high as 2 Mbps in stationary user environments, employing a 5 MHz channel width. Moreover, HSDPA technology further increases the throughput speeds, providing theoretical data rates as high as 14Mbps.WiMAX is becoming a serious threat for 3G cellular networks because of its broadband and distance capabilities, as well as its ability to effectively support voice with full Quos. WiMAX is also able to offer higher data rates than UMTS, but it does not allow the same grade of mobility. However, it is expected to be set up as an alternative to cellular networks, as

the investments the operators need to carry out for its deployment are not so high.

1.10 WIMAX Advantages

- ***Flexible Architecture:***

WiMAX supports several system architectures, including Point-to-Point, Point-to-Multipoint, and ubiquitous coverage. The WiMAX MAC (Media Access Control) supports Point-to-Multipoint and ubiquitous service by scheduling a time slot for each Subscriber Station (SS). If there is only one SS in the network, the WiMAX Base Station (BS) will communicate with the SS on a Point-to-Point basis. A BS in a Point-to-Point configuration may use a narrower beam antenna to cover longer distances.

- ***High Security:***

WiMAX supports AES (Advanced encryption Standard) and 3DES (Triple DES, where DES is the Data Encryption Standard). By encrypting the links between the BS and the SS, WiMAX provides subscribers with privacy (against eavesdropping) and security across the broadband wireless interface. Security also provides operators with strong protection against theft of service. WiMAX also has built-in VLAN support, which provides protection for data that is being transmitted by different users on the same BS.

- ***WiMAX QOS:***

WiMAX can be dynamically optimized for the mix of traffic that is being carried. Four types of service are supported.

- ***Quick Deployment:***

Compared with the deployment of wired solutions, WiMAX requires little or no external plant construction. For example, excavation to support the trenching of cables is not required.

Operators that have obtained licenses to one of the licensed bands, or that plan to use one of the unlicensed bands; do not need to submit further applications to the Government. Once the antenna and equipment are installed and powered, WiMAX is ready for service. In most cases, deployment of WiMAX can be completed in a matter of hours, compared with months for other solutions.

- ***Multi-Level Service:***

The manner in which QOS is delivered is generally based on the Service Level Agreement (SLA) between the service provider and the end-user. Further, one service provider can offer different SLAs to different subscribers, or even to different users on the same SS.

- ***Interoperability:***

WiMAX is based on international, vendor-neutral standards, which make it easier for end-users to transport and use their SS at different locations, or with different service providers. Interoperability protects the early investment of an operator since it can select equipment from different equipment vendors, and it will continue to drive the costs of equipment down because of mass adoption.

- ***Portability:***

As with current cellular systems, once the WiMAX SS is powered up, it identifies itself, determines the characteristics of the link with the BS, as long as the SS is registered in the system database, and then negotiates its transmission characteristics accordingly.

- ***Mobility:***

The IEEE 802.16e amendment has added key features in support of mobility. Improvements have been made to the OFDM and OFDMA physical layers to support devices and services in a mobile environment. These improvements, which include Scaleable OFDMA, MIMO, and support for idle/sleep mode and hand-off, will allow full mobility at speeds up to 160 km/hr. The WiMAX Forum-supported standard has inherited OFDM's superior NLOS (Non-Line of Sight) performance and multipath-resistant operation, making it highly suitable for the mobile environment.

- ***Cost-effective:***

WiMAX is based on an open, international standard. Mass adoption of the standard, and the use of low-cost, mass-produced chipsets, will drive costs down dramatically, and the resultant competitive pricing will provide considerable cost savings for service providers and end-users.

- ***Wider Coverage:***

WiMAX dynamically supports multiple modulation levels, including BPSK, QPSK, 16-QAM, and 64-QAM. When equipped with a high-power amplifier and operating with a low-level modulation (BPSK or QPSK, for example), WiMAX systems are able to cover a large geographic area when the path between the BS and the SS is unobstructed.

- ***Non-Line-of-Sight Operation:***

NLOS usually refers to a radio path with its first Fresnel zone completely blocked. WiMAX is based on OFDM technology, which has the inherent capability of handling NLOS environments. This capability helps WiMAX products deliver broad bandwidth in a NLOS environment, which other wireless product cannot do.

- ***High Capacity:***

Using higher modulation (64-QAM) and channel bandwidth (currently 7MHz, with planned evolution towards the full bandwidth specified in the (associated IEEE and ETSI standards), WiMAX systems can provide significant bandwidth to end-users.

1.11 WiMAX Applications

WIMAX technology will revolutionize the way we communicate. It will provide total freedom to people who are highly mobile, allowing them to stay connected with voice, data and video services. WiMAX will allow people to go from their homes to their cars, and then travel to their offices or anywhere in the world, all seamlessly. To illustrate the ability of WiMAX to address the applications outlined in the preceding section, several representative usage scenarios, grouped into two broad categories – private and public networks are outlined in the following sections.

1.11.1 Private Networks

Private networks, used exclusively by a single organization, institution or business, offer dedicated communication links for the secure and reliable transfer of voice, data and video. Quick and easy deployment is generally a high priority, and configurations are typically Point-to-Point or Point-to-Multipoint.

1.11.2 Cellular Backhaul

The market for cellular services is becoming more and more competitive. To stay in the business, cellular operators are constantly looking for ways to reduce operating costs. Backhaul costs for cellular operators represent a significant portion of their recurring costs.

WiMAX can provide Point-to-Point links of up to 30 miles (50 km), with data rates capable of supporting multiple E1/T1s Cellular operators can therefore use WiMAX equipment to backhaul Base Station traffic to their Network Operation and **Switching Centers , as shown in *Figure 1.19*.**

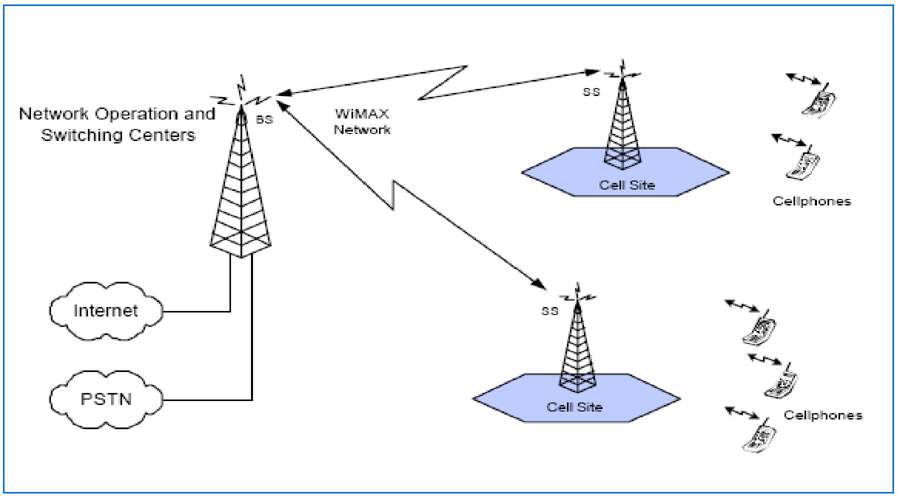


Fig.1.19: *Cellular Backhaul*

Note: *Based on the availability of spectrum for WiMAX in different countries, the cellular backhaul application may or may not be able to handle nationwide networks.*

Cellular traffic is a mix of voice and data, for which the built-in QOS feature of WiMAX is highly suited. Leasing backhaul facilities from local telephone companies can be cost prohibitive, and deploying a fiber solution, which is both costly and time consuming, could negatively impact rollout of service. Wired solutions for providing cellular backhaul are seldom cost-effective in rural or suburban areas, and most versions of DSL and cable technology cannot offer the required bandwidth, especially for backhauling upcoming 3G networks.

1.11.3 Wireless Service Provider Backhaul

Wireless Service Providers (WSPs) use WiMAX equipment to backhaul traffic from Base Stations in their access networks as shown in ***Figure 1.20***.

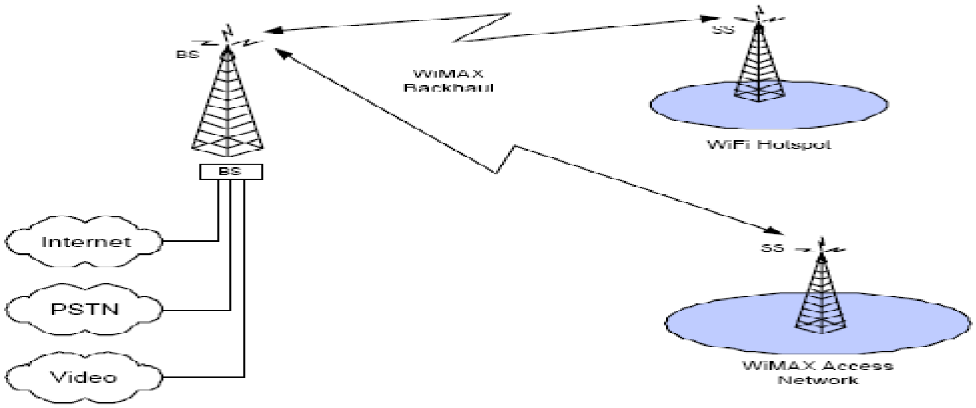


Fig.1.20: Wireless Service Provider Backhaul

Access networks may be based on Wi-Fi, WiMAX or any proprietary wireless access technology. If the access network uses Wi-Fi equipment, the overall WSP network is referred to as a Hot Zone. Since WSPs typically offer voice, data and video, the built-in QOS feature of WiMAX will help prioritize and optimize the backhauled traffic. WiMAX equipment can be deployed quickly, facilitating a rapid rollout of the WSP network.

As already illustrated, leasing backhaul facilities from the local telephone company will increase operating costs, and deployment of a fiber solution can be very costly and requires significant lead times, negatively impacting rollout. Furthermore, fiber, DSL and cable are not cost-effective in rural and suburban areas, and most versions of DSL and cable technology will not provide the capacity required for these networks.

1.11.4 Banking Networks

Large banks can connect branches and ATM sites to their regional office through a private WiMAX network carrying voice, data and video traffic, as shown in ***Figure 1.21*** These banks are normally spread over a large area and need high security and bandwidth to handle the traffic.

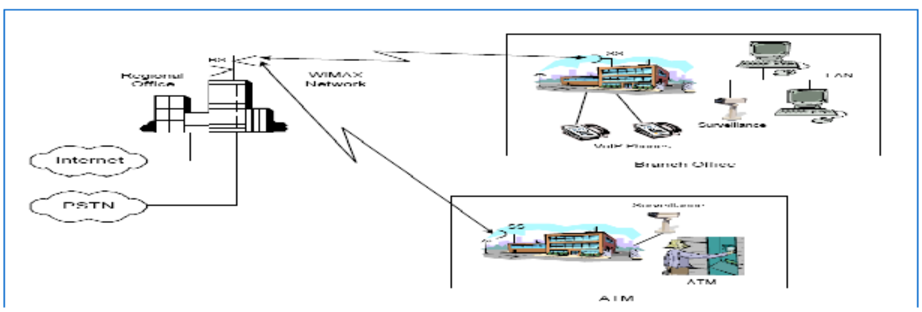


Fig.1.21: Banking Networks

WiMAX data encryption offers excellent link security, however, banks will most likely also need end-to-end security, such as that provided by SSL, to protect against undesired interception and manipulation of sensitive banking traffic.

The broad coverage and high capacity allows the bank's regional office to be connected to a large number of diversely located brand offices and ATM sites. WiMAX networks also offer a high degree of scalability, so that low-data-rate traffic between the regional office and ATM machines can co-exist with the high levels of traffic needed to support branch-to-regional office communications. The WiMAX QOS, which is used to prioritize voice (telephony among branches), data (financial transactions, email, Internet, and intranet) and video (surveillance, CCTV) traffic make this possible. It is desirable for banks to own their own networks, for a number of reasons.

Besides eliminating the repeat costs charged by telephone companies, this will provide banks the ability to quickly redeploy their network if an ATM or branch is temporarily or permanently relocated. In addition to their inability to be quickly deployed, most versions of DSL and cable technology will not provide the bandwidth required to support and sustain branch-to-regional office communications.

1.11.5 Education Networks

School boards can use WiMAX networks to connect schools and school board offices within a district, as shown in ***Figure 1.22***. Some of the key requirements for a school system are NLOS, high bandwidth (>15 Mbps), Point-to-Point and Point-to-Multipoint capability, and a large coverage footprint.

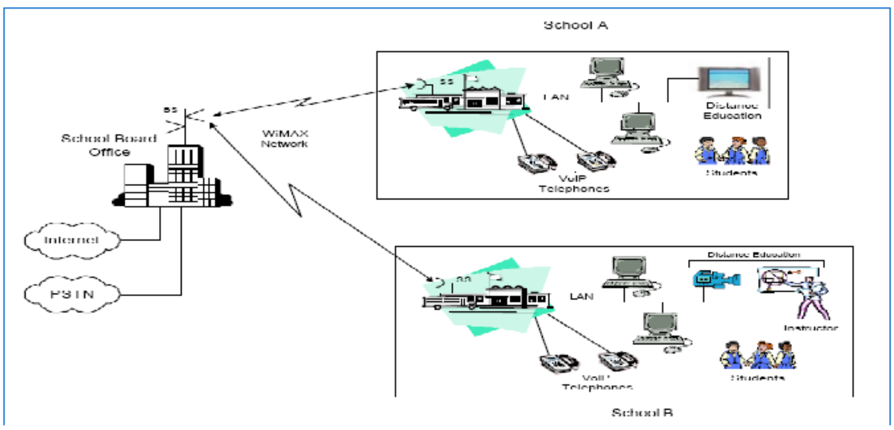


Fig.1.22: *Education Networks*

WiMAX based education networks, using QOS, can deliver the full range of communication requirements, including telephony voice, operating data (such as student records), email, Internet and intranet access (data), and distance education (video)between the school board office and all of the schools in the school district, and between the schools themselves.

In the above scenario, the camera at School B delivers real-time classroom instruction to School A, allowing the schools to simultaneously deliver instruction from a recognized subject-matter expert to a large number of students, eliminating the need for additional instructors. The WiMAX solution provides broad coverage, making it very cost-effective, particularly for rural schools, which may have little or no communications infrastructure, and which are widely dispersed. When school boards.

Own and operate their own network, they can be responsive to changes in the location and layout of their facilities. This will significantly reduce the annual operating cost of leased lines. Wired solutions cannot offer a quickly deployable, low-cost solution, and most versions of DSL and cable technology do not have the throughput required by these education networks.

1.11.6 Public Safety

Government public safety agencies, such as police, fire, and search and rescue, can use WiMAX networks to support response to medical and other emergency situations, as shown in ***Figure 1.23***.

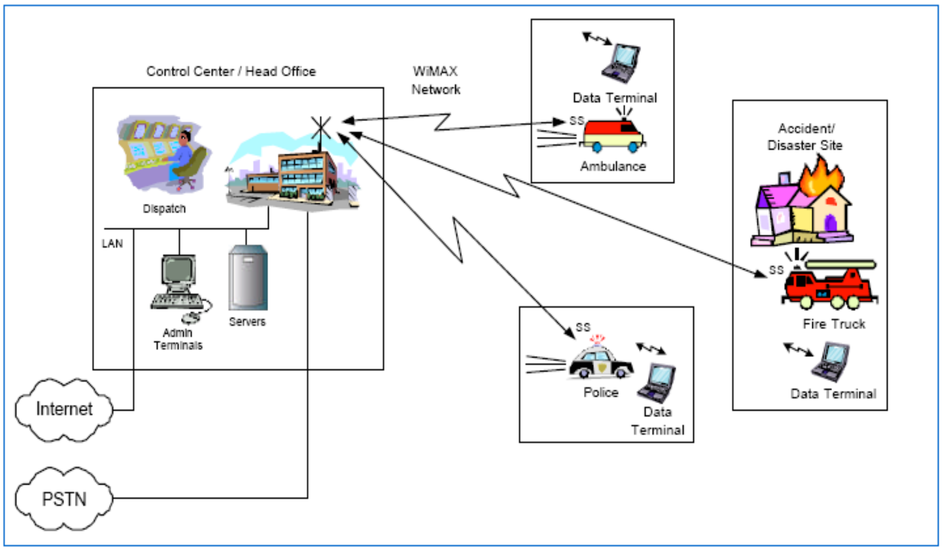


Fig.1.23: *Public Safety*

1.10.7 Offshore Communications

Oil and gas producers can use WiMAX equipment to provide communication links from land-based facilities to oilrigs and platforms, to support remote operations, security, and basic communications, as shown in ***Figure 1.24***.

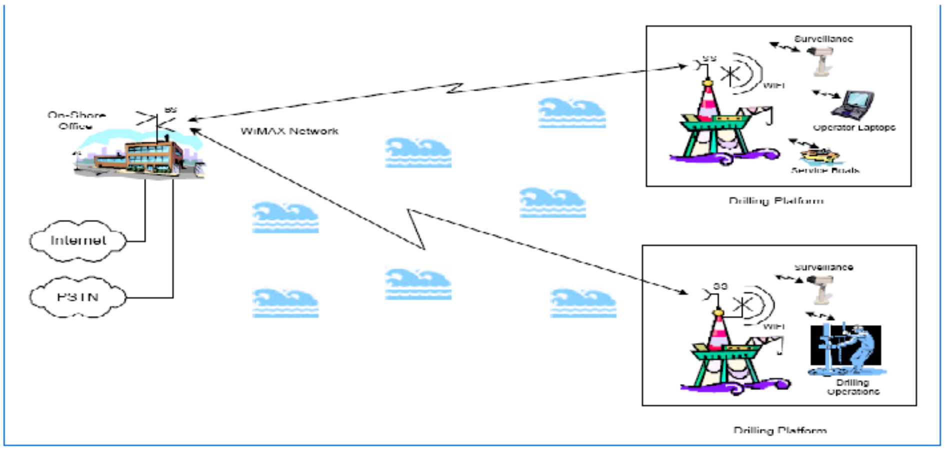


Fig.1.24: *Offshore Communications*

Remote operations include remote troubleshooting of complex equipment problems, site monitoring, and database access. For example, video clips of malfunctioning components or subassemblies can be transmitted to a land-based team of experts for analysis.

Security includes alarm monitoring and video surveillance. Basic communications includes voice telephony, email, Internet access, and video conferencing. WiMAX networks are quickly and easily deployed.

The network can be set up or redeployed in a matter of hours, if not minutes, even when oilrigs and platforms are moved to other locations. Wired solutions are not appropriate for this scenario, because the facilities are offshore, and since oilrigs are temporarily located and moved regularly within the oil or gas field. In the event of having to temporarily abandon an offshore facility, communications for monitoring the status of the asset can continue to be maintained, using battery-backed WiMAX terminals.

1.11.8 Campus Connectivity

Government agencies, large enterprises, industrial campuses, transportation hubs, universities, and colleges, can use WiMAX networks to

connect multiple locations, sites and offices within their campus, as shown in ***Figure 1.25***.

Campus systems require high data capacity, low latency, a large coverage footprint, and high security. Like other usage scenarios, campus networks carry a mix of voice, data, and video, which the WiMAX QOS helps prioritize and optimize.

It takes less time and resources to interconnect a campus through a WiMAX network, since excavation and external construction are not required. Some campuses have been around for a long time, and digging trenches for cable may not be permitted. In such cases, WiMAX solutions may be one of the most effective ways to interconnect campus buildings.

Even if wired installations are permitted, the lead-time to deploy a wired solution is much longer than the lead-time to deploy a WiMAX solution, without offering any accompanying benefits.

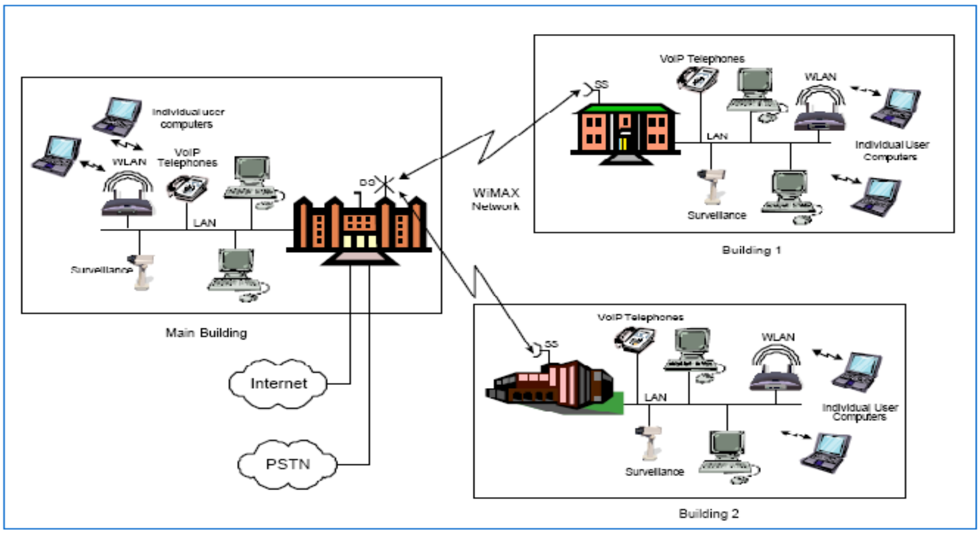


Fig.1.25: *Campus Connectivity*

1.11.9 Temporary Construction Communications

Construction companies can use WiMAX networks to establish communication links between the company head office, construction sites, offices of other project participants, such as architectural and engineering firms, and storage facilities, as shown in ***Figure 1.26.***

The fast deploy ability of WiMAX networks is also important in this scenario, since it allows for quick provision of communications to the

construction site, including voice (telephony) and data (emails, engineering drawings, and Internet access). Surveillance video can also be carried over the network to support monitoring of the site or areas of the site that are otherwise difficult to access. A local Hotspot can also be set up at the construction site, allowing personnel at the site to communicate and exchange data and schedule information. Like the other usage scenarios, the WiMAX built-in QOS will prioritize network traffic and optimize the communications channel. Construction sites include, but are not limited to, office buildings, residential land development, and oil and gas facilities. Since construction activity at these sites is temporary, wired solutions are usually not appropriate. WiMAX equipment, being highly portable, can be redeployed and reused at other construction sites.

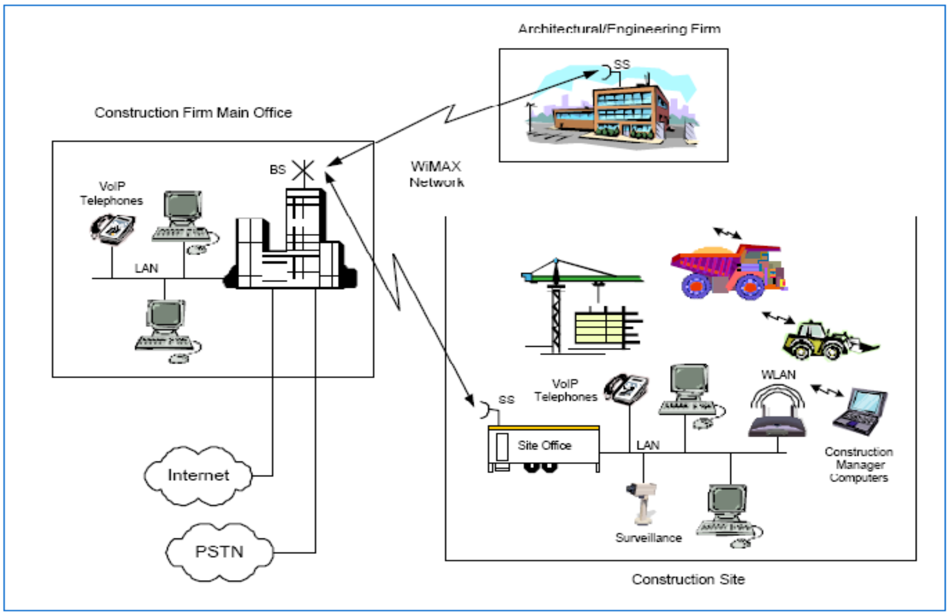


Fig.1.26: *Temporary Construction Communications*

1.11.10 Theme Parks

Theme park operators can use WiMAX to deliver a broad range of communication services for their amusement parks, expositions, hospitality and operation censers, and buses and service vehicles, as shown in ***Figure 1.27***.The above network can support a wide range of communications traffic, including two-way dispatch from a control center, video surveillance throughout the park, reservation data, inventory database access and update, site status monitoring, video on demand, and voice telephony. Some of the key requirements for a system like this are support for fixed and mobile operations, high security, scalable architecture and low latency.

The broad coverage range of WiMAX means an entire park can be covered from only 11 number of Base Stations, scalable upwards as capacity requirements increase. The WiMAX QOS MAC will prioritize and optimize the communications channel, based on the operator's requirements. Re-deployment of the network, in response to changes in theme park facilities, is straightforward and simple, unlike the changes that would be required had the park been served by wired facilities, such as DSL or cable. WiMAX mobility capability will support two-way voice and data communications to the theme park's tour buses and service vehicles. Real-time video can be broadcast to tour buses, providing tourist information, promotions, and weather to passengers.

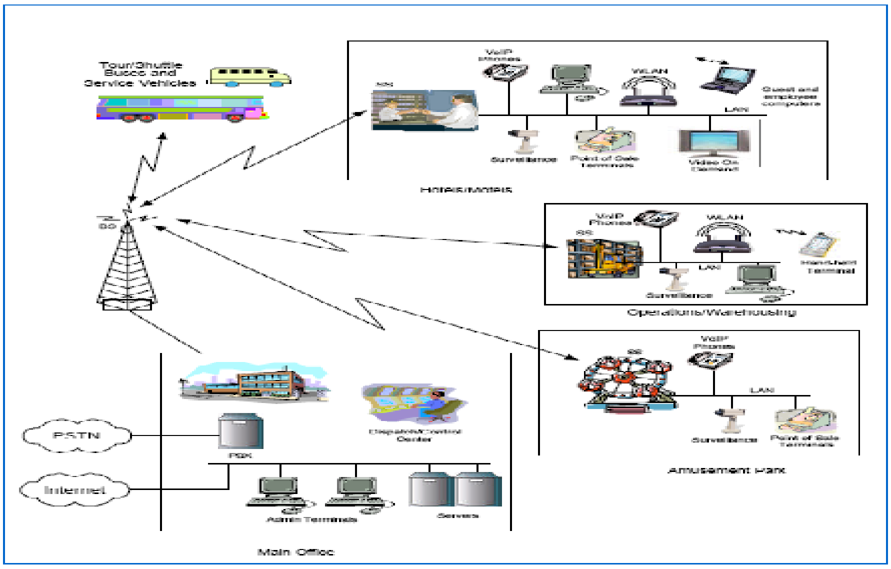


Fig.1.27: Theme Parks

1.11.11 Public Networks

In public network, resources are accessed and shared by different users, including both businesses and private individuals. Public networks generally require a cost-effective means of providing ubiquitous coverage, since the location of the users is neither predictable nor fixed. The main applications of public networks are voice and data communication, although video communication is becoming increasingly popular.

Security is a critical requirement, since many users share the network. Built-in VLAN support and data encryption address these concerns. Several usage scenarios involving public networks.

1.11.12 Wireless Service Provider Access Network

Wireless Service Providers (WSPs) use WiMAX networks to provide connectivity to both residential (voice, data and video) and business (primarily voice and Internet) customers, as shown in ***Figure 1.28***.

The WSP could be a CLEC (Competitive Local Exchange Carriers) that is starting its business with little or no installed infrastructure. Since WiMAX is easy to deploy, the CLEC can quickly install its network and be in position to compete with the ILEC (Incumbent Local Exchange Carrier). The WiMAX built-in QOS mechanism is highly suited for the mix of traffic carried by the CLEC. The QOS MAC also offers multi-level service to address the variety of customer service needs. A common network platform, offering voice, data and video, is highly attractive to end customers, because it presents a one-stop shop and a single monthly bill.

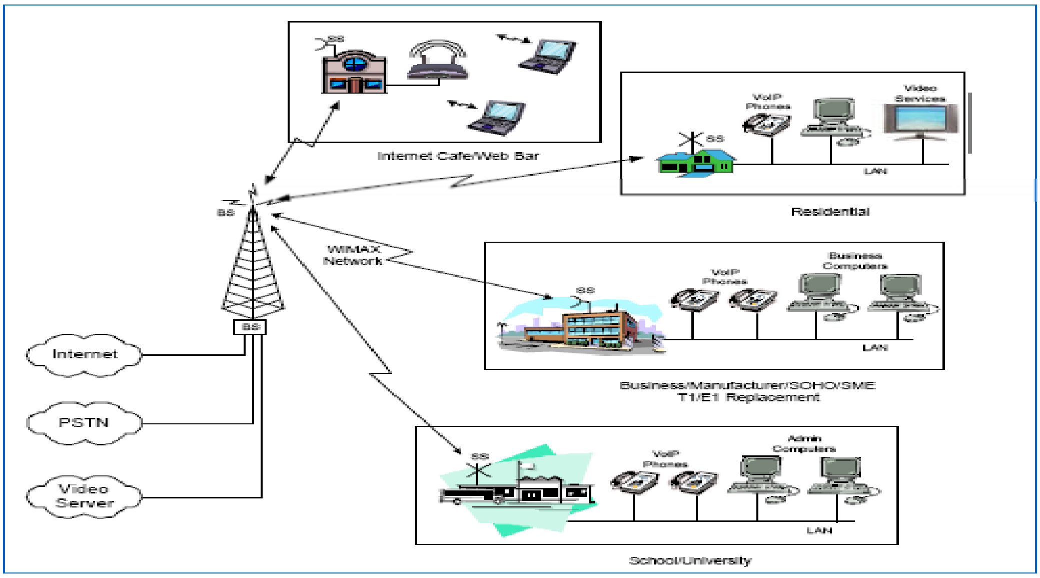


Fig.1.28: *Wireless Service Provider Access Network*

Support for multiple service types allows for different revenue streams, yet it reduces customer acquisition cost, and increases ARPU (Average Revenue Per User). The WSP needs only one billing system and one customer database. Cellular operators may also be interested in applying WiMAX in their networks. These operators already have towers, billing infrastructure and a customer base in place, but the deployment of a WiMAX solution will expand their market presence in their service area.

All of the wired solutions, including fiber, DSL, and cable, require substantial up-front costs for implementing the wired infrastructure. In particular, wired solutions are not suited for markets in developing countries,

where there is very little infrastructure, or in the less-populated areas of developed countries, such as rural areas, small towns or the suburban edges of major centers.

1.11.13 Rural Connectivity

Service providers use WiMAX networks to deliver service to underserved markets in rural areas and the suburban outskirts of cities, as shown in ***Figure 1.29***.The delivery of rural connectivity is critical in many developing countries and underserved areas of developed countries, where little or no infrastructure is available. Rural connectivity delivers much-needed voice telephony and Internet service, since the WiMAX solution. It provides extended coverage; it is a much more cost-effective solution than wired technology in areas with lower population densities.

WiMAX solutions can be deployed quickly, providing communication links to these underserved areas, providing more secure environment, and helping to improve their local economies.

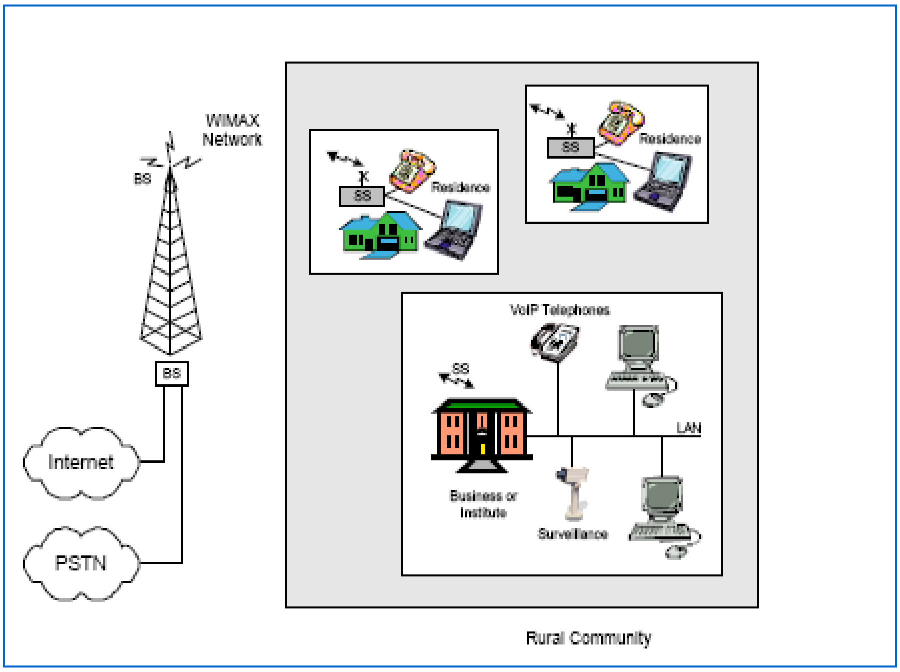


Fig.1.29: *Rural Connectivity*

1.12 Book contents

An overview of the WiMAX system has already been exposed in the present chapter, where the main features of the standard are summarized. In order to understand the objectives and the applications of this system, a comparison between WiMAX and other wireless systems is also included in the chapter.

In chapter 2 presented OFDM, and how OFDM work, and a comparison between OFDM and FDM, TDM, TDMA, OFDMA and the advantage and disadvantage of OFDM.

In chapter 3 presented the IEEE 802.16 protocol and the meaning of PHY layer and why we need it and in this section the supported access provision air interface technologies for different WiMAX profiles are elaborated. In the same chapter we explain MAC layer and the MAC layer consists and how MAX layer work, and what the mobile WiMAX standard IEEE 802.16e requirements in MAC layer.

In chapter 4 presented the PHY layer WiMAX transmitted and receiver and the block diagram of system and explain each block why we need it and representation the theory of action of each block in Tx & Rx.

In chapter 5 presented the security and the types of security and explain briefly the DES *(data encryption standard)* and the standard of theory action of it.

In chapter 6 presented the implementation of PHY layer WiMAX Tx & Rx by VHDL and, explain how we can programmable each block by VHDL and the simulation of each block.

In chapter 7 presented the conclusion of project and the suggestions of future work.

Overview of OFDM

Chapter 2

2.1 Introduction to OFDM

2.1.1 History of OFDM

Orthogonal frequency-division multiplexing, or **OFDM**, is a process of digital modulation that is used in communication technology today. During the last few years wireless communication system has been transferred from low data-rate system to high data-rate system containing of voice, images and even to videos.

The goal of third and fourth generation mobile networks is to provide users with a high data rate, and to provide a wider range of services, such as voice communications, videophones, and high speed Internet access. The higher data rate of future mobile networks will be achieved by increasing the amount of spectrum allocated to the service and by improvements in the spectral efficiency **OFDM** is a potential candidate for the physical layer of fourth generation mobile systems. This thesis presents techniques for improving the spectral efficiency of **OFDM** systems applied in WLAN and mobile networks.

The history of **OFDM** goes back to the 1960's. At the time, there was a need to make more efficient use of bandwidth transmissions without creating situations where signals would be subject to a phenomenon referred to as crosstalk.

The concept dates back some 40 years. This brief history of **OFDM** cites some landmark dates.

At 1960: The **OFDM** technique was used in several high-frequency military systems such as KINEPLEX, ANDEFT, and KATHRYN.

At 1966: Chang shows that multicarrier modulation can solve the multipath problem without reducing data rate. This is generally considered the first official publication on multicarrier modulation. Some earlier work was Hollinger's 1964 MIT dissertation and some of Gallager's early work on water filling.

At 1971: Weinstein and Ebert show that multicarrier modulation can be accomplished using a DFT.

At 1985: Cimini at Bell Labs identifies many of the key issues in **OFDM** transmission and does a proof-of-concept design.

At 1993: DSL adopts **OFDM**, also called discrete multitone, following successful field trials/competitions at Bellcore versus equalizer-based systems.

At 1999: The IEEE 802.11 committee on wireless LANs releases the 802.11a standard for **OFDM** operation in 5GHz UNI band.

At 2002: The IEEE 802.16 committee releases an **OFDM** based standard for wireless broadband access for metropolitan area networks under revision 802.16a.

At 2003: The IEEE 802.11 committee releases the 802.11g standard for operation in the 2.4GHz band.

At 2004: The multiband **OFDM** standard for ultra-wideband is developed, showing **OFDM** usefulness in low SNR systems.

2.1.2 What is OFDM?

Orthogonal Frequency Division Multiplexing **OFDM** is a multicarrier modulation technique that has recently found wide adoption in a widespread variety of high-data-rate communication systems, including digital subscriber lines, wireless LANs (802.11a/g/n), digital video broadcasting, and now WiMAX (802.16e/f/g/k) and other emerging wireless broadband systems.

OFDM is one of the applications of a parallel-data-transmission reduces the influence of multipath fading and makes complex equalizers unnecessary as shown in **Figure 2.1**.

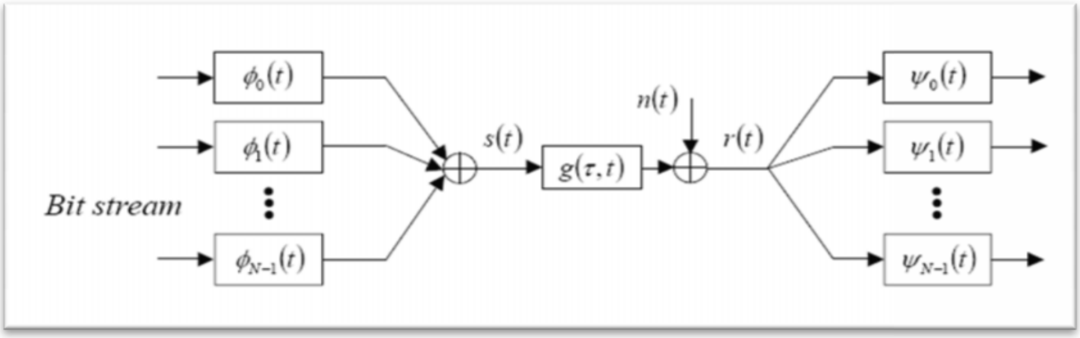


Fig.2.1: Conceptual scheme of a multi-carrier transmission system

OFDM is one of the applications of a parallel-data-transmission reduces the influence of multipath fading and makes complex equalizers unnecessary as shown in **Figure 2.2**.

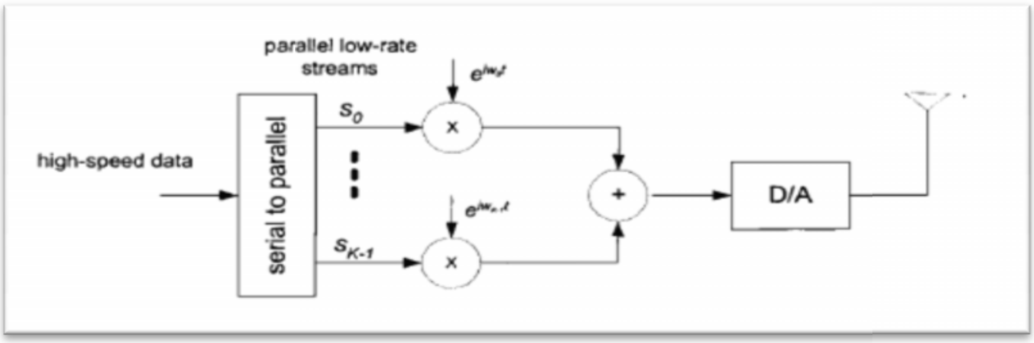


Fig.2.2: parallel-data-transmission scheme

In **OFDM** systems, the spectrum of individual subcarrier is overlapped with minimum frequency spacing, which is carefully designed so that each subcarrier is orthogonal to the other subcarriers. The bandwidth efficiency of **OFDM** is another advantage as shown in **Figure 2.3**.

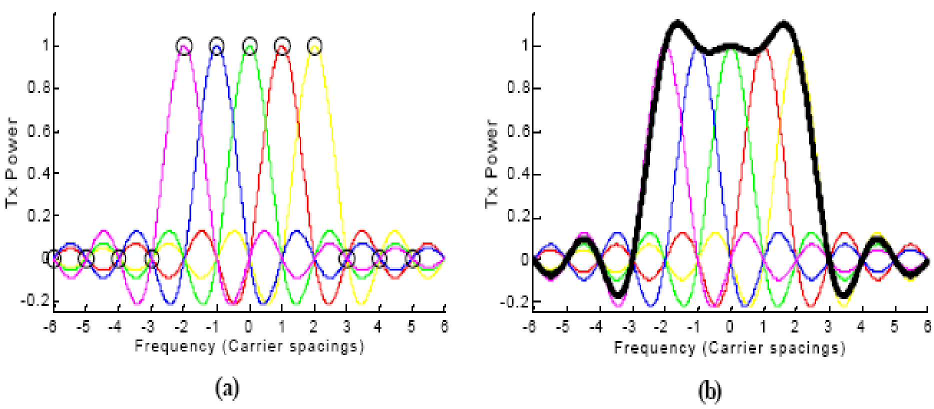


Fig.2.3: Frequency response of the subcarriers in a 5 tone OFDM signal

OFDM is a multiplexing technique that subdivides the bandwidth into multiple frequency sub-carriers.

In an **OFDM** system, the input data stream is divided into several parallel sub-streams of reduced data rate (thus increased symbol duration) and each sub-stream is modulated and transmitted on a separate orthogonal sub-carrier.

OFDM can be viewed as either a modulation technique or a multiplex technique. In case of Modulation technique, it viewed by the relation between input and output signals. On the other hand from Multiplex technique, **OFDM** is viewed as the output signal which is the linear sum of the modulated signal.

OFDM is a method of using many carrier waves instead of only one, and using each carrier wave for only part of the message.

OFDM uses the principles of **FDM** to allow multiple messages to be sent over a single radio channel. It is however in a much more controlled manner, allowing an improved spectral efficiency.

Each carrier in an **OFDM** signal has a very narrow bandwidth (i.e. 1 kHz), thus the resulting symbol rate is low. This results in the signal having a high tolerance to multipath delay spread, as the delay spread must be very long to cause significant inter-symbol interference (e.g. > 100 ms).

2.1.3 Advantages and Disadvantages of OFDM

Advantages:

- Immunity to delay spread and multipath, Robust against Inter-symbol interference **(ISI)** and fading caused by multipath propagation.
- Resistance to frequency selective fading.
- Simple equalization, Robust against narrow-band co-channel interference.
- Efficient bandwidth usage, High spectral efficiency.
- Robust against Inter-symbol interference **(ISI)** and fading caused by multipath propagation.
- Efficient implementation using FFT.
- Tuned sub-channel receiver filters are not required (unlike conventional **FDM**).

- Multiuser diversity, **OFDMA** allows different users to transmit over different portions of the broadband spectrum (traffic channel).
- Receiver simplicity, **OFDMA** has the merit of easy decoding at the receiver side, as it eliminates the intra-cell interference avoiding CDMA type of multi-user detection.

Disadvantages:

- Sensitive to carrier frequency offset and phase noise .
- The Peak-to-Average Ratio **(PAG)** which tends to reduce the power efficiency of the radio frequency **(RF)** amplifier.
- Sensitive to Doppler shift.
- Nonlinear effects generated by the power amplifier may introduce intercarrier- interference and thus destroy the orthogonality.

2.1.4 Comparison among different multiplexing techniques

2.1.4.1 OFDM versus FDM

OFDM is different from **FDM** in several ways. In conventional broadcasting each radio station transmits on a different frequency, effectively using **FDM** to maintain a separation between the stations. There is however no coordination or synchronization between each of these stations.

With an **OFDM** transmission such as Digital Audio Broadcasting **(DAB)**, the information signals from multiple stations are combined into a single multiplexed stream of data. This data is then transmitted using an **OFDM** ensemble that is made up from a dense packing of many subcarriers. All the subcarriers within the **OFDM** signal are time and frequency synchronized to each other, allowing the interference between subcarriers to be carefully controlled.

These multiple subcarriers overlap in the frequency domain, but do not cause Inter-Carrier-Interference **(ICI)** due to the orthogonal nature of the modulation.

Typically with **FDM** the transmission signals need to have a large frequency guard-band between channels to prevent interference. This lowers the overall spectral efficiency. However with **OFDM** the orthogonal packing

of the subcarriers greatly reduces this guard band, improving the spectral efficiency.

In **FDM** the total signal frequency band is divided into *N* non-overlapping frequency subchannel. Each subchannel is modulated with a separate symbol, and then the *N* sub channels are frequency multiplexed. It seems good to avoid spectral overlap of channels to eliminate interchannel interference. However, this leads to inefficient use of the available spectrum.

OFDM use parallel data and **FDM** with overlapping subchannel, in which each, carrying a signaling rate *b,* is spaced *b* apart in frequency to avoid the use of high-speed equalization and to combat impulsive noise and multipath distortion, as well as to use the available bandwidth fully.

Show the difference between the conventional non-overlapping multicarrier technique and the overlapping multicarrier modulation technique.

By using the overlapping multicarrier modulation technique, we save almost 50% of bandwidth. To realize this technique, however, we need to reduce cross talk between SCs, which means that we want orthogonality between the different modulated carriers, this overcomes the problem of overhead carrier spacing required in **FDMA**.

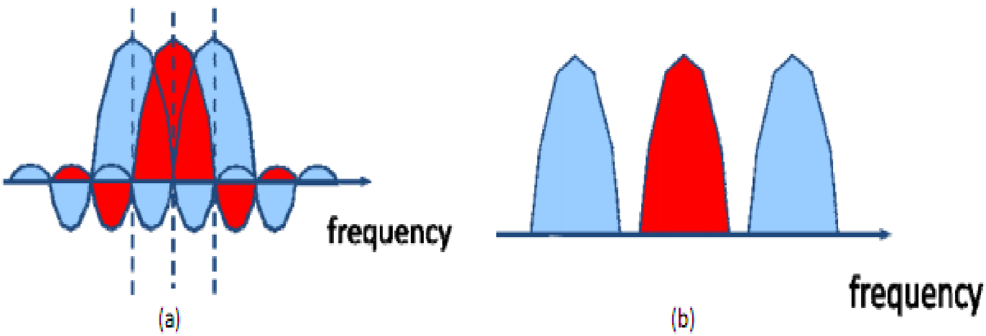


Fig.2.4: *Concept of the OFDM signal:*
(a) Conventional multicarrier technique (FDM).
(b) Orthogonal multicarrier modulation technique (OFDM).

2.1.4.2 OFDM Versus TDM

TMD systems transmit data in a buffer and burst method, thus the transmission of each channel is non-continuous. The input data to be

transmitted is buffered over the previous frame and burst transmitted at a higher rate during the time slot for the channel.

TDMA cannot send analog signals directly due to the buffering required, thus are only used for transmitting digital data. **TDMA** can suffer from multipath effects as the transmission rate is generally very high, resulting in significant Intersymbol interference.

There is an overhead associated with the change over between users due to time slotting on the channel. A change B over time must be allocated to allow for any tolerance in the start time of each user, due to propagation delay variations and synchronization errors. This limits the number of users that can be sent efficiently in each channel. In addition, the symbol rate of each channel is high (as the channel handles the information from multiple users) resulting in problems with multipath delay spread as shown in **Figure 2.5.**

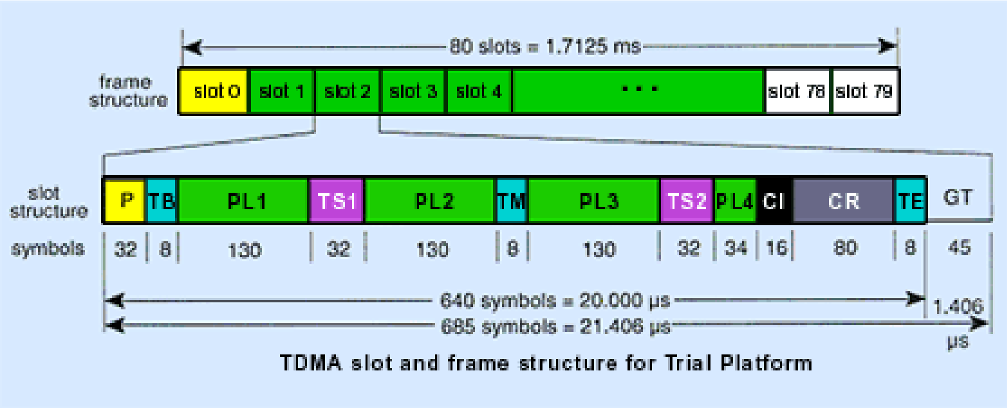


Fig.2.5: TDMA scheme where each user is allocated a small time slot

OFDM exploits the frequency diversity of the multipath channel by coding and interleaving the information across the sub-carriers prior to transmissions. Complex equalizers are not required to compensate for frequency selective fading.

OFDMA therefore, is very well-suited to support smart antenna technologies. The increased symbol duration improves the robustness of **OFDM** to delay spread.

Furthermore, the introduction of the cyclic prefix (CP) can completely eliminate Inter-Symbol Interference **(ISI)** as long as the CP duration is longer than the channel delay spread. **OFDM** splits the available bandwidth into many narrow band channels (typically 100-8000).

Because of this there is no great need for users to be time multiplex as in **TDMA**, thus there is no overhead associated with switching between users.

2.1.4.3 OFDM versus CDMA

The **CDMA** signal is generated by modulating the data by the PN sequence. The modulation is performed by multiplying the data (XOR operator for binary signals) with the PN sequence as shown in **Figure 2.6**.

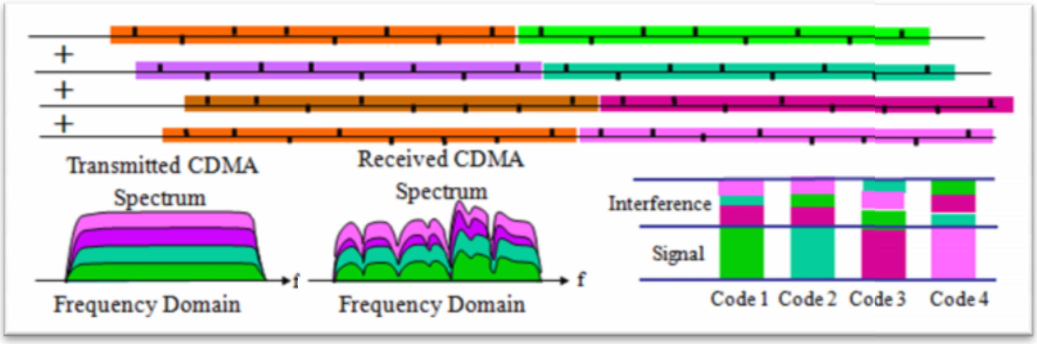


Fig.2.6: *Conventional CDMA PN Code sequence*

CDMA is achieved by modulating the data signal by a pseudo random noise sequence (PN code), which has a chip rate higher than the bit rate of the data. The PN code sequence is a sequence of ones and zeros.

CDMA can suffer from two problems, Near Far Problem (NFP) so in **CDMA** cellular, the base station uses a fast closed-loop power control scheme to tightly control each mobile's transmit power, And the other problem *Multiple Access Interference* (MAI) These PN sequences are statistically uncorrelated, and the sum of a large number of PN sequences results in *Multiple Access Interference* (MAI) that is approximated by a Gaussian noise process. If all of the users are received with the same power level, then the variance (e.g., the noise power) of the MAI increases in direct proportion to the number of users.

At **OFDMA** the carriers for each channel are made orthogonal to one another, allowing them to be spaced very close together.

OFDM was found to perform very well compared with **CDMA**, with it out-performing **CDMA** in many areas for a single and multi-cell environment. **OFDM** was found to allow up to 2-10 times more users than **CDMA** in a single cell environment and from 0.7 – 4 times more users in a multi-cellular environment. The difference in user capacity between **(OFDM)** and **CDMA** was dependent on whether cell sectorization and voice activity detection is used.

2.1.5 Applications

- Broadcasting
  - ❖**DAB** (Digital Audio Broadcasting)
  - ❖**DVB** (Digital Video Broadcasting)

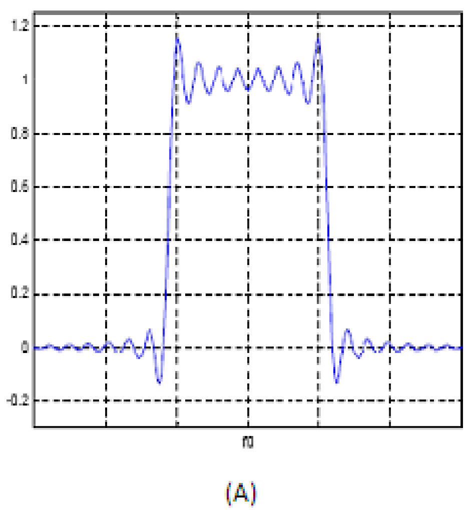
- WLAN (Wireless Local Area Networks)
  - ❖IEEE 802.11a
  - ❖HiperLAN/2

- Wireless MAN (Wireless Metropolitan Area Networks)
  - ❖IEEE 802.16 (WiMAX)

2.2 Basics of OFDM

2.2.1 Orthogonality

The subcarriers are orthogonal to each other when we multiply the waveforms of any two subcarriers and integrate over the symbol period the result is zero. The orthogonality of the carriers means that each carrier has an integer number of cycles over a symbol period. Due to this, the spectrum of each carrier has a null at the centre frequency of each of the other carriers in the system as shown in **Figure 2.7**.



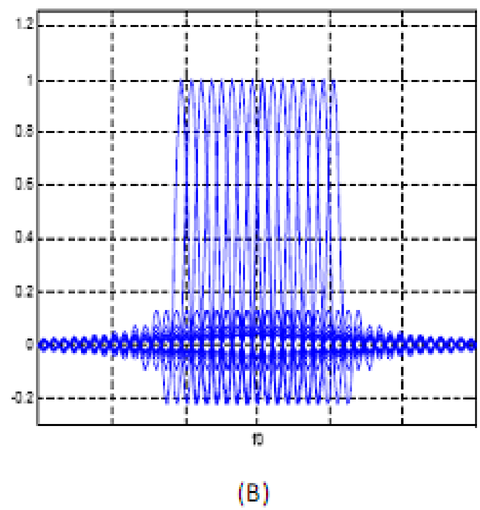


Fig.2.7: *(A) Basis functions of an OFDM signal with N=16 carriers represented in frequency domain*
(B) Resulting spectrum from the basic functions.

This results in no interference between the carriers, allowing then to be spaced as close as theoretically possible. This overcomes the problem of overhead carrier spacing required in **OFDM**.

Signals are orthogonal if they are mutually independent of each other. Orthogonality is a property that allows multiple information signals to be transmitted perfectly over a common channel and detected without interference.

OFDM achieves orthogonality in the frequency domain by allocating each of the separate information signals onto different subcarriers.

OFDM signals are made up from a sum of sinusoids, with each corresponding to a sub carrier.

The base band frequency of each sub carrier is chosen to be an integer multiple of the inverse of the symbol time, resulting in all subcarriers having an integer number of cycles per symbol. As a consequence the subcarriers are orthogonal to each other.

Sets of functions are orthogonal to each other if they match the conditions in equation. If any two different functions within the set are multiplied, and integrated over a symbol period, the result is zero, for orthogonal functions.

$$\int_0^T S_i(t)\, S_j(t)dt = \begin{cases} c & i = j \\ 0 & i \neq j \end{cases}$$

Another way of thinking of this is that if we look at a matched receiver for one of the orthogonal functions, a sub carrier in the case of **OFDM**, then the receiver will only see the result for that function. The results from all other functions in the set integrate to zero, and thus have no effect, and equation shows a set of orthogonal sinusoids, which represent the subcarriers for an unmodulated real **OFDM** signal.

$$S_k(t) = \begin{cases} \sin(2\pi k f_0 t) & 0 < t < T \quad k = 1,2,3 \cdots M \\ 0 & Otherwise \end{cases}$$

Where:

f_0 is the carrier spacing ,

M is the number of carriers,

T is the symbol period.

Since the highest frequency component is **Mf_0** the transmission bandwidth is also **Mf_0** .

Figure 2.8 shows the construction of an **OFDM** signal with four subcarriers. **(1a), (2a), (3a)** and **(4a)** show individual subcarriers, with 1, 2, 3, and 4 cycles per symbol respectively. The phase on all these subcarriers is zero.

Note that each sub carrier has an integer number of cycles per symbol making them cyclic. Adding a copy of the symbol to the end would result in a smooth join between symbols

(1b), **(2b)**, **(3b)** and **(4b)** show the FFT of the time waveforms in **(**1a**)**, **(2a), (3a)** and **(4a)** respectively. **(4a)** and **(4b)** shows the result for the summation of the 4 sub carriers.

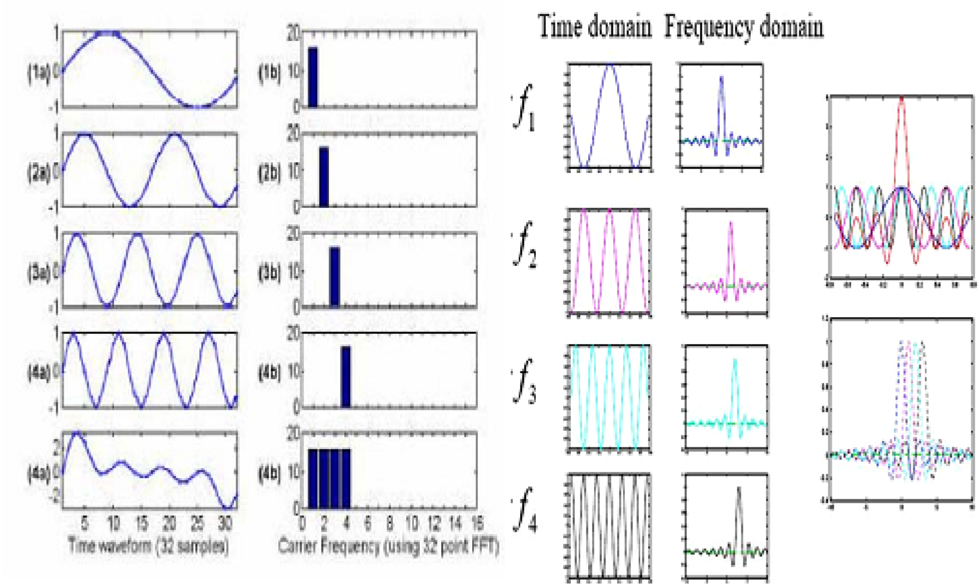


Fig.2.8: Time domain construction of an OFDM signal

This results in sum and difference frequency components, which will always be integer sub carrier frequencies, as the frequency of the two mixing subcarriers has integer number of cycles. Since the system is linear we can integrate the result by taking the integral of each frequency component separately then combining the results by adding the two sub integrals.

The two frequency components after the mixing have an integer number of cycles over the period and so the sub-integral of each component will be zero, as the integral of a sinusoid over an entire period is zero.

Both the sub-integrals are zeros and so the resulting addition of the two will also be zero, thus we have established that the frequency components are orthogonal to each other. Orthogonal frequency division multiplexing is then

the concept of typically establishing a communications link using a multitude of carriers each carrying an amount of information identical to the separation between the carriers.

A more detailed understanding of Orthogonal arises when we observe that the bandwidth of a modulated carrier has a so called "Sinc" shape with nulls spaced by the bit rate. In **OFDM**, the carriers are spaced at the bit rate, so that the carriers fit in the nulls of the other carriers. Another view of Orthogonal is that each carrier has an integer number of sine wave cycles in one bit period.

2.2.2 Cyclic Prefix

The increased symbol duration in **OFDMA** improves the delay spread while the Inter Symbol Interference **(ISI)** is completely eliminated by introduction of a Cyclic Prefix (some data). CP is a repetition of the last samples of the data portion that is appended at the beginning of the data payload.

The ISI is completely eliminated as long as the CP duration is longer than the channel delay spread. A drawback of the CP is that it introduces overhead, which effectively reduces bandwidth efficiency. Since **OFDM** signal power spectrum has a sharp fall off at the edge of channel, a larger fraction of the allocated channel bandwidth can be utilized for data transmission which compensates the loss in efficiency due to the cyclic prefix. The concept of CP in **OFDMA** is explained as shown in **Figure 2.9**.

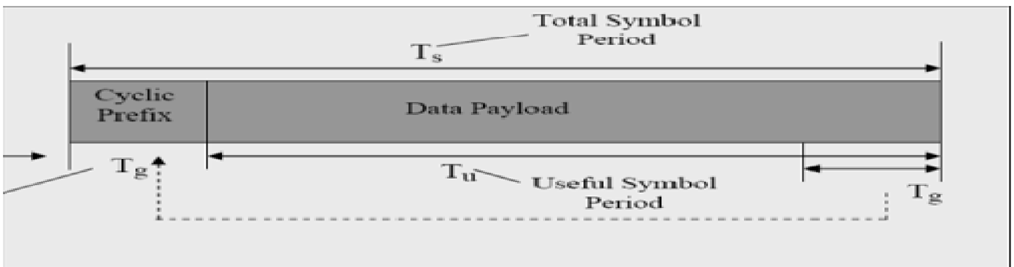


Fig.2.9: Cyclic Prefix in OFDM

The total length of the symbol is $T_S = T_G + T_{FFT}$, where T_S the total length of the symbol in samples is, T_G the length of the guard period in samples, and T_{FFT} the size of the IFFT used to generate the OFDM signal.

The strength of **OFDM** is maximized by the introduction of a guard period among the transmitted symbols. The guard period allows time for multi-path signals from the earlier symbol to gradually disappear before the information

from the present symbol is get together. Cyclic extension is the most essential guard to period to employ. Cyclic extension is necessary to decode the symbol by using the FFT. This satisfies the multi-path resistance and the symbol time synchronization tolerance.

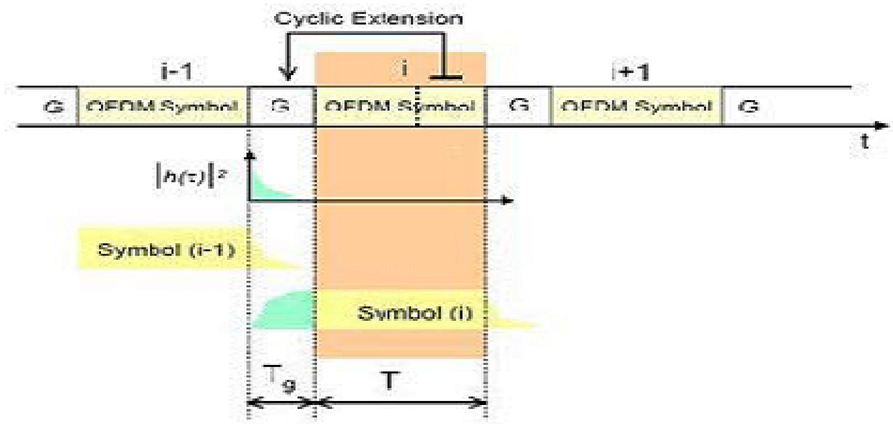


Fig.2.10: *Cyclic Prefix in OFDM*

For a given system bandwidth the symbol rate for an **OFDM** signal is much lower than a single carrier transmission scheme. For example for a single carrier **BPSK** modulation, the symbol rate corresponds to the bit rate of the transmission.

However for OFDM the system bandwidth is broken up into N_C subcarriers, resulting in a symbol rate that is N_C times lower than the single carrier transmission. This low symbol rate makes **OFDM** naturally resistant to effects of Intersymbol Interference **(ISI)** caused by multipath propagation.

Multipath propagation is caused by the radio transmission signal reflecting off objects in the propagation environment, such as walls, buildings, mountains, etc. These multiple signals arrive at the receiver at different times due to the transmission distances being different. This spreads the symbol boundaries causing energy leakage between them. The effect of ISI on an **OFDM** signal can be further improved by the addition of a Cyclic Prefix to the start of each symbol. This guard period is a cyclic copy that extends the length of the symbol waveform.

Each subcarrier, in the data section of the symbol, (i.e. the **OFDM** symbol with no guard period added, which is equal to the length of the IFFT size used to generate the signal) has an integer number of cycles. Because of these placing copies of the symbol end-to-end results in a continuous signal, with no

discontinuities at the joins. Thus by copying the end of a symbol and appending this to the start results in a longer symbol time.

2.2.3 Multiple Accesses in OFDM

Multiple access schemes are used to allow many simultaneous users to use the same fixed bandwidth radio spectrum. In any radio system, the bandwidth that is allocated to it is always limited. For mobile phone systems the total bandwidth is typically 50 MHz, which is split in half to provide the forward and reverse links of the system.

Sharing of the spectrum is required in order increase the user capacity of any wireless network. **FDMA**, **TDMA** and **CDMA** are the three major methods of sharing the available bandwidth to multiple users in wireless system. There are many extensions, and hybrid techniques for these methods, such as **OFDMA**, and hybrid **TDMA** and **FDMA** systems.

However, an understanding of the three major methods is required for understanding of any extensions to these methods.

OFDMA is similar to **FDMA** in that the multiple user access is achieved by subdividing the available bandwidth into multiple channels, which are then allocated to users as shown in **Figure 2.11**. However, **OFDMA** uses the spectrum much more efficiently by spacing the channels much closer together. This is achieved by making all the carriers orthogonal to one another, preventing interference between the closely spaced carriers.

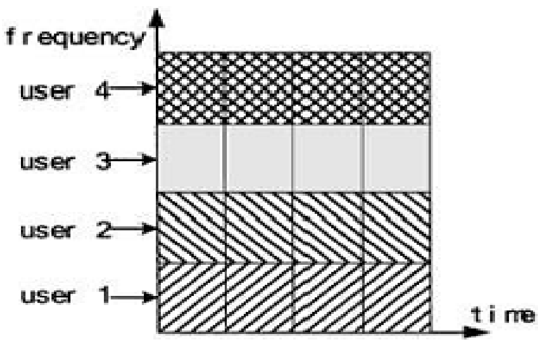


Fig.2.11: *FDMA channelization*

Before the digital implementation of **OFDMA**, **FDMA** can only be realized using multiple analog RF modules if one terminal is occupying multiple frequency bands. **FDMA** therefore was deemed unsuitable for broadband communications. However, the rise of **OFDM**, and in particular, its

IFFF/FFT implementation, give **FDMA** a new life as a broadband multiple access scheme.

The use of IFFF /FFT allows terminals to arbitrarily combine multiple frequencies (subcarriers) at the baseband, leading to orthogonal frequency division multiple access (**OFDMA**) scheme as shown in **Figure 2.12**.

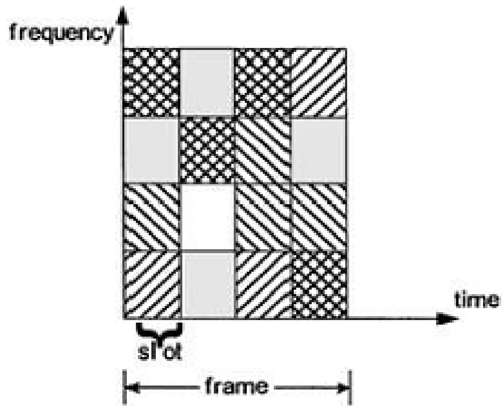


Fig.2.12: *OFDMA channelization*

An **OFDMA** system is defined as one in which each terminal occupies a subset of subcarriers (termed an **OFDMA** traffic channel), and each traffic channel is assigned exclusively to one user at any time PI.

In **OFDMA**, users are not overlapped in frequency domain at any given time. However, the frequency bands assigned to a particular user may change over the time as shown in **Figure 2.12**.

The IEEE 802.16a-e has an **OFDMA** mode with bandwidth options of 1.25, 5**,** 10 or 20 MHz depending on the bandwidth, the entire spectrum is divided into 128, 512, 1024 or 2048 subcarriers.

For example, a 20 MHz band with 2048-FFT yields a subcarrier spacing of 9.8 KHz. In time domain, the resource is further divided into frames and sub frames that can be allocated to different users.

2.2.4 OFDM versus Single Carrier

Orthogonal frequency division multiplexing **(OFDM)** technology provides operators with an efficient means to overcome the challenges of NLOS propagation. The WiMAX **OFDM** waveform offers the advantage of being

able to operate with the larger delay spread of the NLOS environment. By virtue of the **OFDM** symbol time and use of a cyclic prefix, the **OFDM** waveform eliminates the inter-symbol interference **(ISI)** problems and the complexities of adaptive equalization. Because the **OFDM** waveform is composed of multiple narrowband orthogonal carriers, selective fading is localized to a subset of carriers that are relatively easy to equalize.

An example is shown in **Figure 2.13** and **Figure 2.14** as a comparison between an **OFDM** Multi carrier signal and a single carrier signal, with the information being sent in parallel for **OFDM** and in series for single carrier.

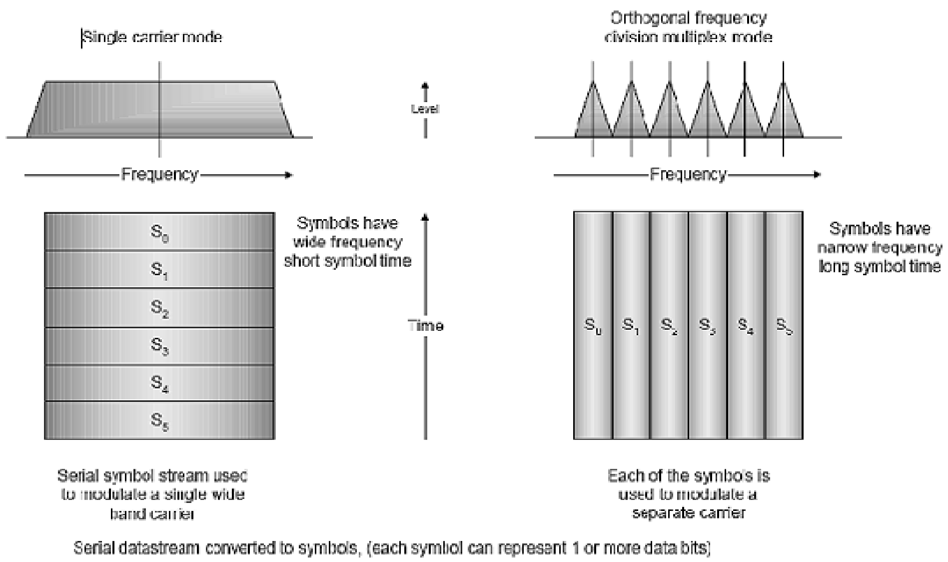


***Fig.2.13:** Single carrier and OFDM*

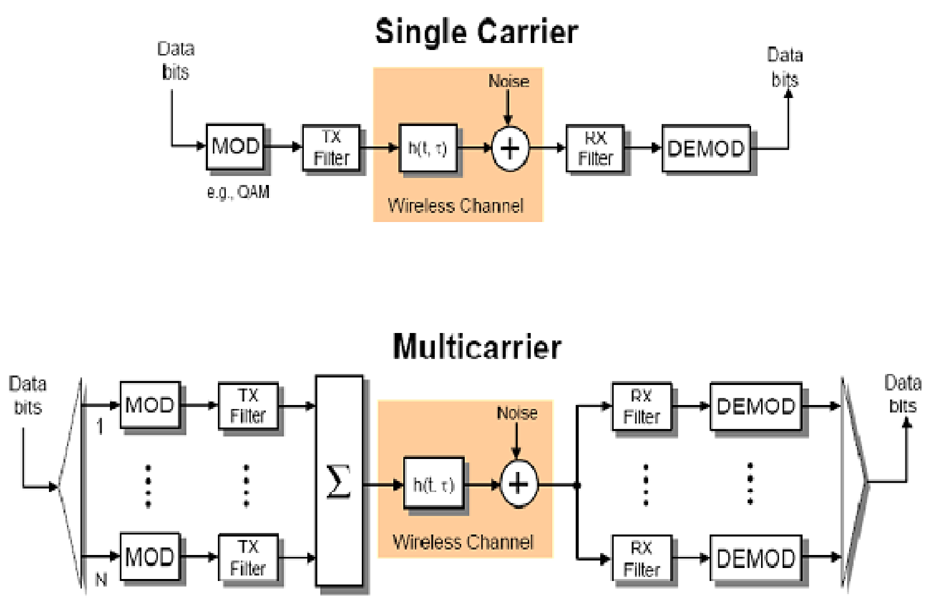


***Fig.2.14:** Single carrier and OFDM*

The ability to overcome delay spread, multi-path, and ISI in an efficient manner allows for higher data rate throughput. As an example it is easier to equalize the individual **OFDM** carriers than it is to equalize the broader single carrier signal as shown in **Figure 2.15** and **Figure 2.16**.

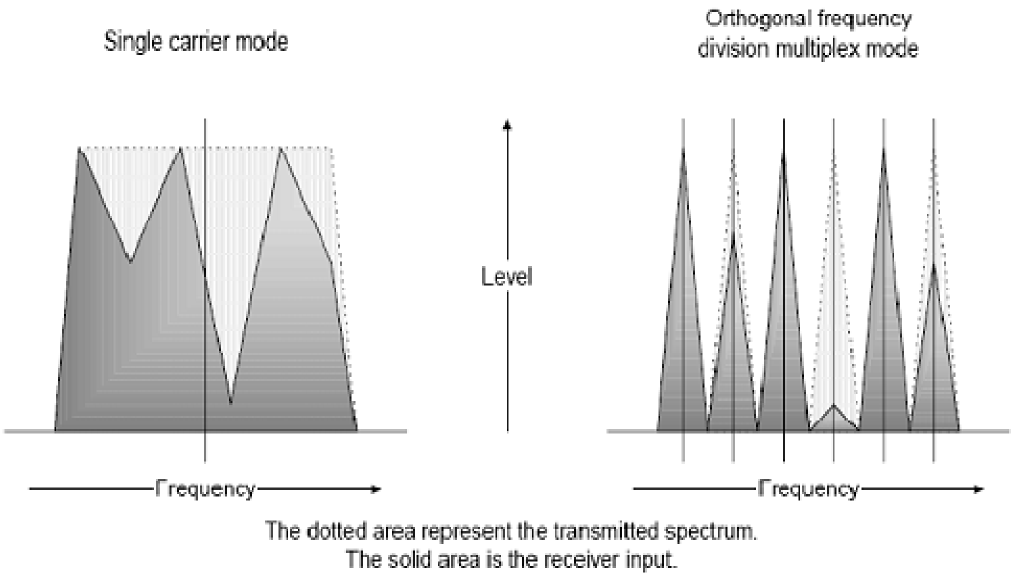


Fig.2.15: *Single carrier and OFDM received*

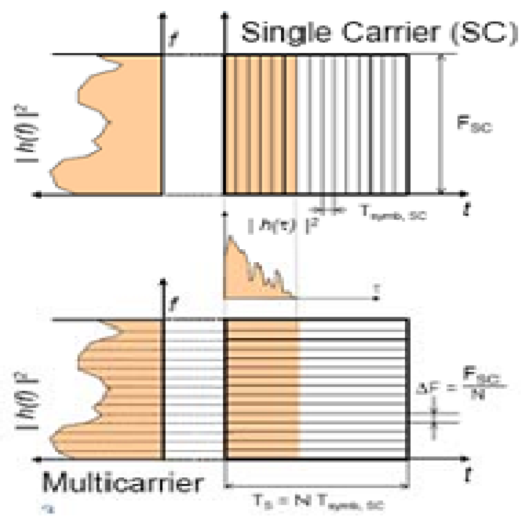


Fig.2.16: *Single carrier and OFDM*

In radio transmissions, the channel spectral response is not flat. In the frequency domain large delay spreads translate into frequency-selective fading. Signals on some frequencies arrive at the receiver in phase while signals at some other frequencies arrive out of phase. This results in *"frequency selective fading"* as shown in Figure 2.17. NLOS channels may also vary in time significantly, due to moving transceivers in mobile communications. Also time

variation of NLOS channels is caused by other moving objects in the paths of signals. This results in time selective fading as shown in **Figure 2.17**.

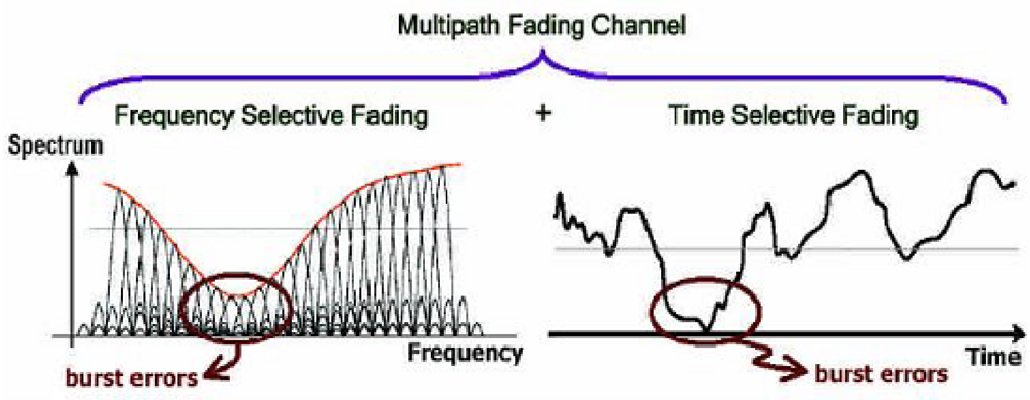


Fig.2.17: Multi path Fading Channel

The **OFDMA** symbol structure consists of three types of sub-carriers as shown in **Figure 2.18**.

- Data sub-carriers for data transmission.
- Pilot sub-carriers for estimation and synchronization purposes.
- Null sub-carriers for no transmission; used for guard bands and DC carriers.

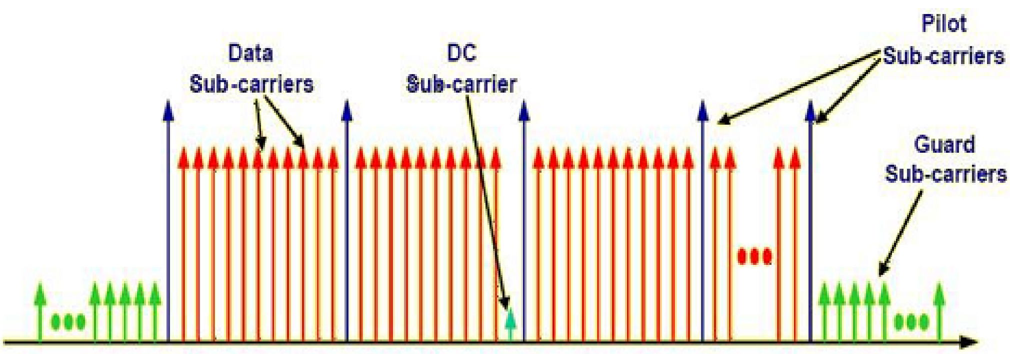


Fig.2.18: OFDM sub carrier structure

Active (data and pilot) sub-carriers are grouped into subsets of sub-carriers called subchannels. The WiMAX **OFDMA** PHY supports sub-channelization in both DL and UL.

The minimum frequency-time resource unit of sub channelization is one slot, which is equal to 48 data tones (sub-carriers).

There are two types of sub-carrier permutations for sub-channelization; diversity and contiguous. The diversity permutation draws sub-carriers pseudo-

randomly to form a subchannel. It provides frequency diversity and inter-cell interference averaging.

2.2.5 Scalable OFDM Access (SOFDMA)

Scalable **OFDMA** is the **OFDMA** mode is used in Mobile WiMAX defined in IEEE 802.16e. Scalability is supported by adjusting the size of FFT size while fixing the sub-carrier frequency spacing in 10.94 kHz. It supports channel bandwidths ranging from 1.25 MHz to 20 MHz.

SOFDMA adds scalability to **OFDMA**. With bandwidth scalability, Mobile WiMAX technology can comply with various frequency regulations worldwide.

When designing **OFDMA** wireless systems the optimal choice of the number of subcarriers per channel bandwidth is a tradeoff between protection against multipath, Doppler shift, and design cost/complexity.

Increasing the number of subcarriers leads to better immunity to the inter-symbol interference **(ISI)** caused by multipath (due to longer symbols); on the other hand it increases the cost and complexity of the system (it leads to higher requirements for signal processing power and power amplifiers with the capability of handling higher peak-to-average power ratios).

Having more subcarriers also results in narrower subcarrier spacing and therefore the system becomes more sensitive to Doppler shift and phase noise.

2.2.5.1 Advantages and Disadvantages of SOFDMA System

Advantages

1. Combating **ISI** and Reducing **ICI**

When signal passes through a time-dispersive channel, the orthogonality of the signal can be lost. CP helps to maintain orthogonality between the sub carriers. Initially guard interval-empty space between two **OFDM** symbols served as a buffer for the multi path reflection. But the empty guard time introduces Inter Carrier Interference **(ICI)** that is crosstalk between different sub carriers. A better solution is cyclic extension of OFDM symbol or CP. It ensures that the delayed replicas of the **OFDM** symbols will always have a complete symbol within the FFT interval (often referred as FFT window).

At the receiver side, CP is removed before any processing starts. As long as the length of CP interval is larger than maximum expected delay spread, all reflections of previous symbols are removed and orthogonality is restore.

2. Spectral Efficiency

In the case of **OFDM**, a better spectral efficiency is achieved by maintaining orthogonality between the sub-carriers.

Disadvantages

1. Strict Synchronization Requirement

OFDMA is highly sensitive to time and frequency synchronization errors. Demodulation of an **OFDM** signal with an offset in the frequency can lead to a high bit error rate.

2. Peak-to-Average Power Ratio (PAPR)

Peak to Average Power Ratio (PAPR) is proportional to the number of subcarriers used for **OFDM** systems. An **OFDM** system with large number of sub-carriers will thus have a very large PAPR when the sub-carriers add up coherently. Large PAPR of a system makes the implementation of Digital-to-Analog Converter **(DAC)** and Analog-to Digital Converter **(ADC)** to be extremely difficult. The design of RF amplifier also becomes increasingly difficult as the PAPR increases.

2.3 OFDM Parameters

The IEEE 802.16-2004 standard specified **OFDM** as the transmission method for NLOS connections. The **OFDM** signal is made up of many orthogonal carriers, and each individual carrier is digitally modulated with a relatively slow symbol rate. This method has distinct advantages in multipath propagation because, in comparison with the single carrier method at the same transmission rate, more time is needed to transmit a symbol.

The **BPSK**, **QPSK**, **16QAM**, and **64QAM** modulation modes are used, and the modulation is adapted to the specific transmission requirements. Transmission rates of up to 75 Mbps are possible. Unlike WiMAX's "little

brother" WLAN, the bandwidth is not constant and can vary between 1.25 MHz and 28 MHz. In IEEE 802.16-2004, a distinction is made between two methods: **OFDM** and **OFDMA**.

In the normal **OFDM** mode, 200 carriers are available for data transmission and both **TDD** and **FDD** methods are used. In the **OFDMA** mode, various subscribers can be served simultaneously by assigning each subscriber a specific carrier group (subchannelization) that carries the data intended for that subscriber.

The number of carriers is also significantly increased. The 802.16e standard is a further expansion of WiMAX in the frequency range up to 6 GHz with the objective of allowing mobile applications and even roaming. In addition, the number of carriers can vary over a wide range depending on permutation zones and FFT base (128, 512, 1024, and 2048). The Korean standard WiBRO is a special case of 802.16e.

OFDM is a combination of modulation and multiplexing. Multiplexing generally refers to independent signals, those produced by different sources. So it is a question of how to share the spectrum with these users. In **OFDM** the question of multiplexing is applied to independent signals but these independent signals are a sub-set of the one main signal.

In **OFDM** the signal itself is first split into independent channels, modulated by data and then remultiplexed to create the **OFDM** carrier. **OFDM** is a special case of Frequency Division Multiplex (**FDM**). As an analogy, a **FDM** channel is like water flow out of a faucet, in contrast the **OFDM** signal is like a shower. In a faucet all water comes in one big stream and cannot be sub-divided. **OFDM** shower is made up of a lot of little streams.

Think about what the advantage might be of one over the other? One obvious one is that if I put my thumb over the faucet hole, I can stop the water flow but I cannot do the same for the shower. So although both do the same thing, they respond differently to interference.

In **OFDM** system, the subcarriers must be orthogonal. The independent sub-channels can be multiplexed by frequency division multiplexing (FDM), called multi-carrier transmission or it can be based on a code division multiplexing (CDM), in this case it is called multi-code transmission.

2.3.1 Basic Terms in OFDM

The WiMAX standard describes different modes of operation:

- Single Carrier (SC / SCa).
- Orthogonal Frequency Division Multiplex (**OFDM** / **OFDMA**).

OFDM is one step in the evolution of transmitting information over a physical media:

- The easiest way to send information is bit-by-bit in time at one particular carrier frequency. With this method, you start with the first bit, transmit it, send the second bit, transmit it, and so on. This is done by means of **ASK** modulation for example.
- A more complex method is to group a certain number of bits together to form a symbol and then to transmit such symbols symbol-by-symbol. **QPSK** (two bits form 1 **QPSK** symbol) or **16QAM** (four bits form one **16QAM** symbol) are examples of this modulation.

OFDM is an even more complex method of transmitting information over a physical channel. The basic concept is to use *"multiple carriers"* (e.g. 256 carriers) to transmit a large number of symbols at the same time, and distributing information blocks containing a certain number of bits to a certain number of carriers.

Using **OFDM** has many advantages, including high spectrum efficiency, resistance against multipath interference (particularly in wireless communications), and ease of filtering out noise (if a particular range of frequencies is affected by interference, the carriers within that range can be disabled or made to run slower). Also, the upstream and downstream speeds can be varied by allocating a higher or lower number of carriers for each purpose.

An extremely important benefit from using multiple subcarriers is that because each carrier operates at a relatively low bit rate, the duration of each symbol is relatively long. For example, if you send a million bits per second over a single baseband channel, then the duration of each bit must be under a microsecond. This imposes severe constraints on synchronization and removal of *"multipath interference"*.

If the same million bits per second are spread among N subcarriers, the duration of each bit can be extended by a factor of N, and the constraints of timing and multipath sensitivity are greatly relaxed. For moving vehicles, the Doppler Effect on signal timing is another constraint that causes difficulties for some other modulation schemes.

The more complex the technique and the greater the information bandwidth (one parameter is *"bit/Hz"*, which indicates how many useful bits can be transmitted when using 1 Hz bandwidth), the more sensitive the systems are to *"disturbing effects"* (such as fading, noise, transmitter and receiver imperfections).

Overcome these problems, more sophisticated techniques to *"recover errors"* have to be introduced (advanced protocols, multipath receivers such as Rake receivers, high-performance receiver frontends, advanced error coding and error recovery methods such as turbo codes, Viterbi decoders, etc).

2.3.2 Basic OFDM Parameters

In order to describe an **OFDM** system, a number of terms are used to specify the parameters of the physical properties. In The following few words, we will explain and illustrate the basic terms related to **OFDM**.

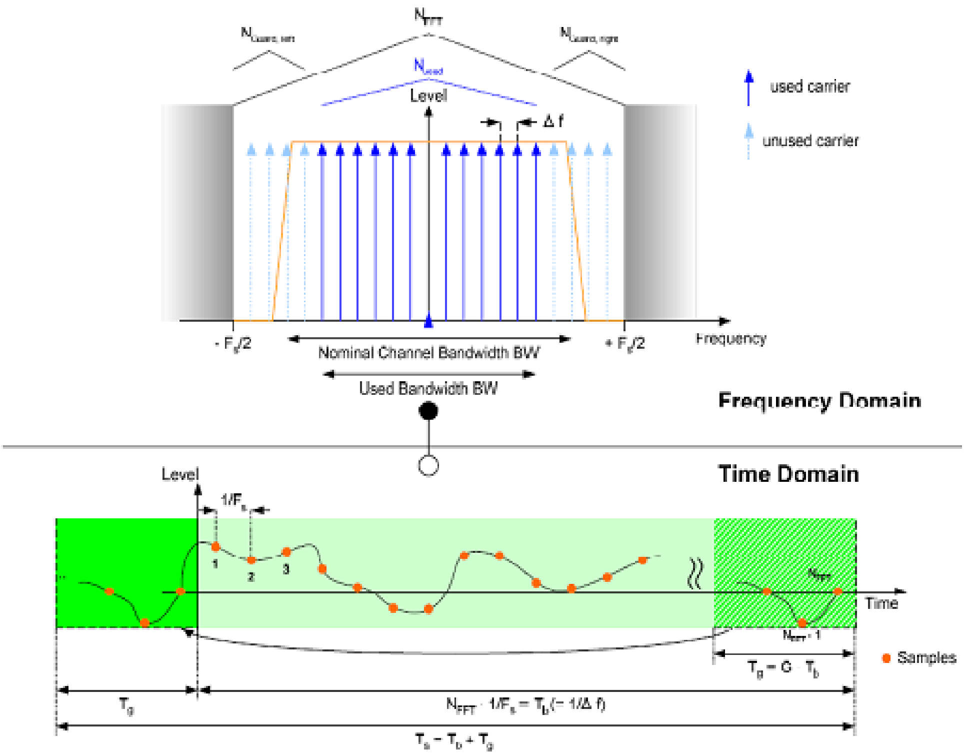


Fig.2.19: *OFDM in Both Time and Frequency domains*

The basic **OFDM** parameters are briefly discussed below, the includes

- **Nominal channel bandwidth BW_n (Hz)**

The bandwidth which is allocated by the governmental authorities Values are 1.5 MHz, 5 MHz or 20 MHz, the bandwidth is defined in **OFDM** as

$$BW_n = \frac{Fs}{n}$$

Where: **Fs** is the sampling frequency,
n is the sampling factor.

- **Used bandwidth BW (Hz)**

The bandwidth is the area which is physically occupied by the WiMAX signal in frequency domain.

$$BW = \Delta f \cdot N_{used}\ (max)$$

Where: **Δf** is the sampling frequency,
N_{used}(max) is the maximum number of used subcarriers.

The used bandwidth must be smaller than the nominal BW.

- **Sampling frequency FS (Hz)**

The sampling frequency is the "core" frequency of the transmission system, that means the frequency at which e.g. of the D/A converter generates new samples.

$$Fs = \frac{\lfloor 8000\ n\ BW \rfloor}{8000}$$

The sampling frequency is always greater that Bandwidth BW.

- **Sampling factor n**

The sampling factor is the ratio of sampling frequency to channel bandwidth.

$$n = \frac{Fs}{BW}$$

*The Typical factors used in **OFDM** are **8/7** (recommended), **28/25, 86/75…etc***

- **FFT size or N_{FFT}**

In **OFDM**, signals are very often processed using fast Fourier transformation (FFT). N_{FFT} Specifies the number of samples for this processing step and is always a power of 2.

*Typical values are **256** (for **OFDM**) or **2048** (for **OFDMA**).*

- **Subcarrier spacing Δf (Hz)**

The distance between two adjacent physical **OFDM** carriers. The value is calculated by Δf that given by

$$\Delta f = \frac{Fs}{N_{FFT}}$$

*For **OFDMA**, this value is e.g. 11.1607 kHz.*

- **Useful symbol time Tb (sec)**

The time a symbol is *"valid"*, which means the correct and undisturbed carrier modulation state (also called the *"orthogonality interval"*) is present, and it can be given as

$$Tb = \frac{1}{S_f}$$

For FFT analysis, this is the analyzed interval length.

- **Guard period ratio / interval G, cyclic prefix (CP) time Tg (sec)**

In order to collect multipath information, a particular ratio of the useful symbol is added to the **OFDM** symbol. This ratio is called *"guard period"* and the absolute time is called *"cyclic prefix"*

$$Tg = G \cdot Tb$$

*Typical values of **G**:* $\frac{1}{4}, \frac{1}{8}, \frac{1}{16}, \frac{1}{32}$

- **(Overall) OFDM symbol time Ts (sec)**

The duration of the complete **OFDM** symbol with useful symbol time and cyclic prefix time, where:

$$Ts = Tb + Tg$$

- **Number of used subcarriers N_{used}**

Due to the shape of the transmission filter, the outer carriers of an **OFDM** signal may be attenuated and thus be disturbed. Also, the DC carrier cannot be used. Consequently, the outer carriers do not carry any modulation data. N_{used} may vary, depending on special transfer modes.

*For **OFDM (NFFT = 256 and N_{used} = 200).***

- **DC subcarrier**

The DC subcarrier is the carrier at the transmission frequency and is not used for data transmission (set to 0).

- **Pilot carriers**

Pilot carriers are used to synchronize the receiver to the transmitter by means of phase, frequency and timing.

***NOTE**: For OFDM, 8 pilot carriers are used.*

- **Guard subcarriers N_{Guard}(left) and N_{Guard} (right)**

The guard subcarriers are the outer carriers, which are not used for transmission.

$$N_{FFT} = N_{used}\,(max) + N_{Guard}\,(left) + N_{Guard}\,(right) + 1\ (DC\ subcarrier)$$

2.3.4 Properties of OFDM

- **Spectrum and performance**

Unshaped QPSK signal produces a spectrum such that its bandwidth is equal to (1+ α) Rs. In **OFDM**, the adjacent carriers can overlap in the manner shown here. The addition of two carriers, now allows transmitting 3Rs over a bandwidth of -2Rs to 2Rs or total of 4Ts. This gives a bandwidth efficiency of 4/3 Hz per symbol for 3 carriers and 6/5 for 5 carriers.

As more and more carriers are added, the bandwidth approaches,

$$\frac{N+1}{N} \text{ bits per Hz.}$$

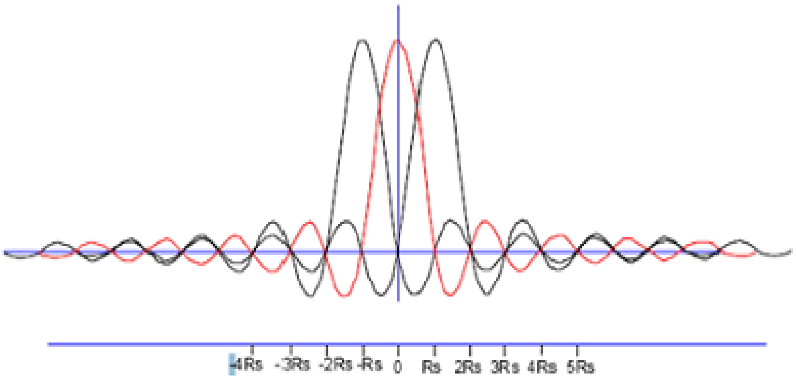


Fig.2.20: *The spectrum of an OFDM signal (Without cyclic prefix)*

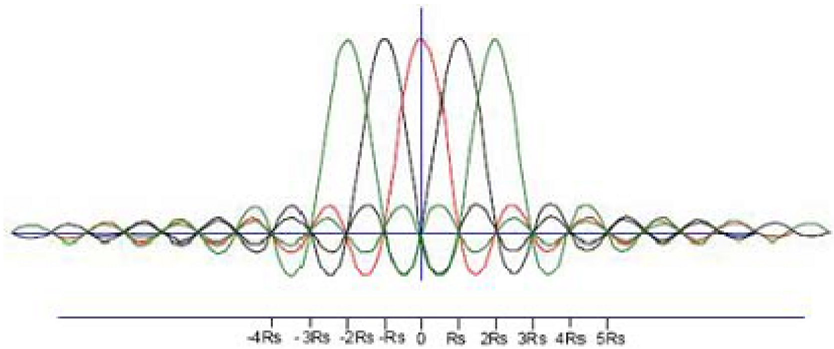


Fig.2.21: *The spectrum of an OFDM signal (without cyclic prefix)*

So the larger the number of carriers, the better. Here is a spectrum of an **OFDM** signal. and note that the out of band signal is down by 50 dB without any pulse shaping.

Comparing this to the spectrum of a QPSK signal, not how much lower the sidebands are for **OFDM** and how much less are the variance.

- **Bit Error Rate performance**

The BER of an **OFDM** is only exemplary in a fading environment. We would not use **OFDM** is a straight line of sight link such as a satellite link. **OFDM** signal due to its amplitude variation does not behave well in a non-linear channel such as created by high power amplifiers on board satellites. Using **OFDM** for a satellite would require a fairly large backoff, on the order

of 3 dB, so there must be some other compelling reason for its use such as when the signal is to be used for a moving user.

- **Peak to average power ratio (PAPR)**

If a signal is a sum of N signals each of max amplitude equal to 1 v, then it is conceivable that we could get max amplitude of N that is all N signals add at a moment at their max points. The PAPR is defined as:

$$R = \frac{|x(t)|^2}{P_{avg}}$$

Where:

R : Peak to average power ratio

x(t) : Peak power

P_{avg} : average power

For an **OFDM** signal that has 128 carriers, each with normalized power of 1 w, then the max PAPR can be as large as log (128) or 21 dB. This is at the instant when all 128 carriers combine at their maximum point, unlikely but possible. The RMS PAPR will be around half this number or 10-12 dB. This same PAPR is seen in CFDM signals as well.

When the signal has to go through amplifier non-linearity. Large back off is required in such cases. This makes use of **OFDM** just as problematic as Multi-carrier FDM in high power amplifier applications such as satellite links.

- **Synchronization**

The other problem is that tight synchronization is needed. Often pilot tones are served in the subcarrier space. These are used to lock on phase and to equalize the channel.

- **Coding**

The sub-carriers are typically coded with convolution coding prior to going through IFFT. The coded version of **OFDM** is called **COFDM** or Coded **OFDM**.

2.3.5 OFDM Real Parameters

The **OFDM** use has increased greatly in the last 10 years. It is now proposed for radio broadcasting such as in Eureka 147 standard and Digital Radio Mondiale (DRM). **OFDM** is used for modem/ADSL application where it coexists with phone line. For ADSL use, the channel, the phone line, is filtered to provide a high SNR. **OFDM** here is called Discrete Multi Tone (DMT.)

(*Remember the special filters on your phone line if you have cable modem*.) **OFDM** is also in use in your wireless internet modem and this usage is called 802.11a. Let's take a look at some parameters of this application of **OFDM**. The summary of these are given below.

- **Data rates**

  6 Mbps to 48 Mbps

- **Modulation**

  BPSK, QPSK, 16 QAM and 64 QAM

- **Coding**

  Convolution concatenated with Reed Solomon

- **FFT size**

  64 with 52 sub-carriers uses, 48 for data and 4 for pilots.

- **Subcarrier frequency spacing**

  20 MHz divided by 64 carriers or .3125 MHz

- **FFT period**

  Also called symbol period, 3.2 μsec = 1/Δf

- **Guard duration**

  One quarter of symbol time, 0.8 μsec

- **Symbol time**

  4 μsec

2.3.6 Subchannelization

As WiMAX is designed to operate as an infrastructure network, resource allocation is also an important topic. Within WiMAX (**OFDM** and **OFDMA**), subchannelization allows you to group the complete number of **OFDM** carriers into blocks and assign each block to a different segment of a base station. The blocks are spread over the complete frequency range and contain a number of adjacent carriers.

The subchannel index controls the use of the different blocks over the entire spectrum.

The complete number of data subcarriers (192) can be divided into 2, 4, 8 or 16 subchannels. All subcarriers are spread in four different "regions" of the available frequency range.

If, four subchannels are used (as in the example below), there will be 16/4 = 4 different subchannel indices and 192/4 = 48 subcarriers per subchannel, which are distributed over four different "regions", thus yielding 48/4 = 12 adjacent subcarriers per subchannel block.

Figure 2.22 below shows the concept of subchannelization with the example of four used subchannels. Subchannel index 12 (green) is used as an example.

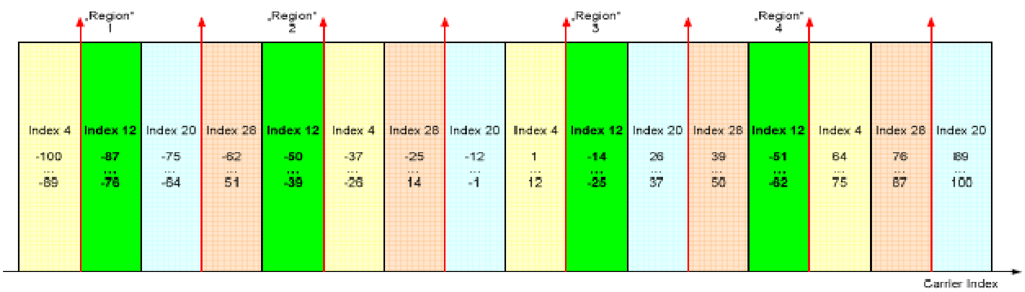


Fig.2.22: Subchannelization with 4 used subchannels

As shown in **Figure 2.23** Subchannelization in the uplink is an option within WiMAX. Without sub channelization, regulatory restrictions and the need for cost effective CPEs, typically cause the link budget to be asymmetrical, this causes the system range to be up link limited. Sub channeling enables the link budget to be balanced such that the system gains are similar for both the up and down links. Subchanneling concentrates the transmit power into fewer **OFDM** carriers; this is what increases the system gain that can either be used to extend the reach of the system, overcome the

building penetration losses, and or reduce the power consumption of the CPE. The use of sub channeling is further expanded in orthogonal frequency division multiple access **(OFDMA)** to enable a more flexible use of resources that can support nomadic or mobile operation.

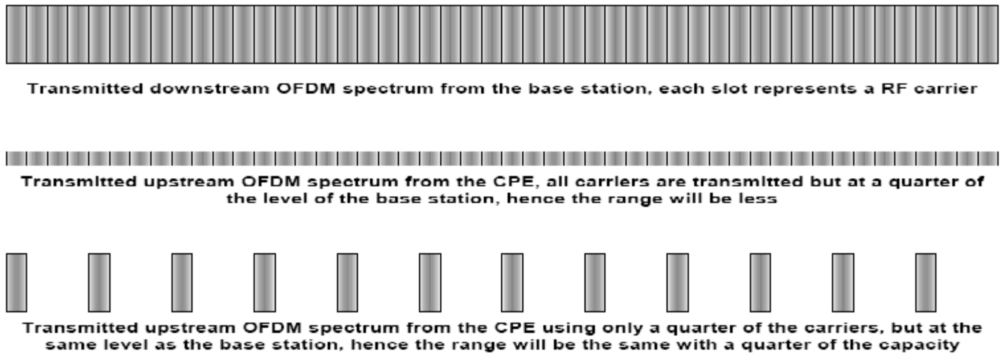


Fig.2.23: *The effect of sub-channelization*

2.3.7 Frame Structure

Frame structure is illustrated in **Figure 2.24** that shows the frame structure of an WiMAX **OFDM** transmission. A frame is divided into a DL and a UL sub frame. The DL and UL sub frames start with the preamble 8 a known symbol with a limited number of carriers 8 to recover information about the transmission channel and allow the receiver to recover the channel response. The FCH and DL MAP contain information about the frame content (location and modulation of the individual bursts) and is BPSK-modulated.

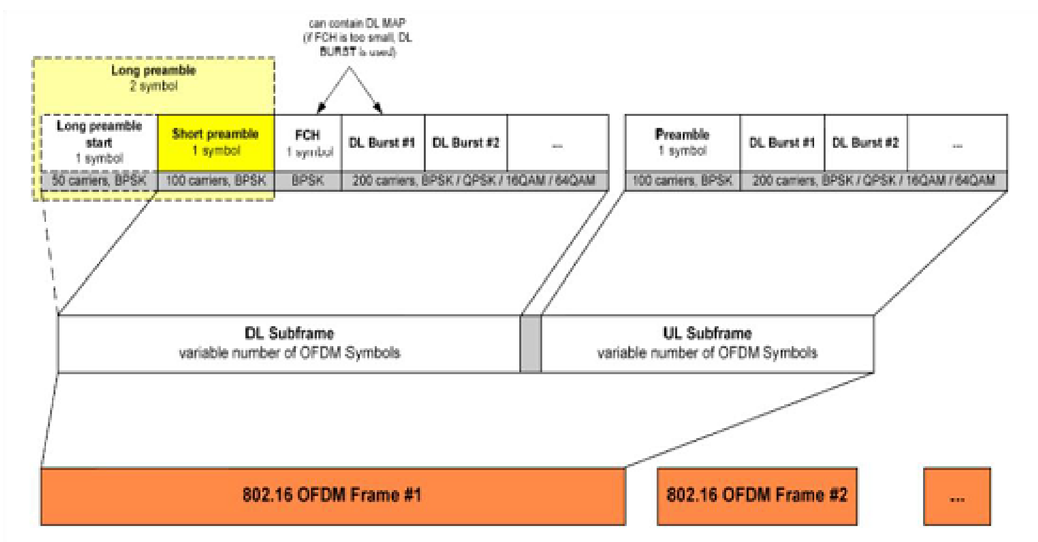


Fig.2.24: *OFDM frame structure*

2.3.8 From Bits to Carrier

To get a basic impression of how **OFDM** / **OFDMA** transmission works, the path from bits to the carrier is described as shown in **Figure 2.25** that shows a 802.16-2004 **OFDM** transmitter (with parts of the **OFDMA** transmitter) and is just an overview; the detailed implementation may vary.

First, data from upper layers pass the randomizer, which converts long 0's or 1's sequences into randomly scrambled data, showing better coding performance in the next steps of transmission. The initialization value consists of the base station ID, DL or UL interval usage code (DIUC/UIUC) and frame number. The randomizer is implemented as a feedback register.

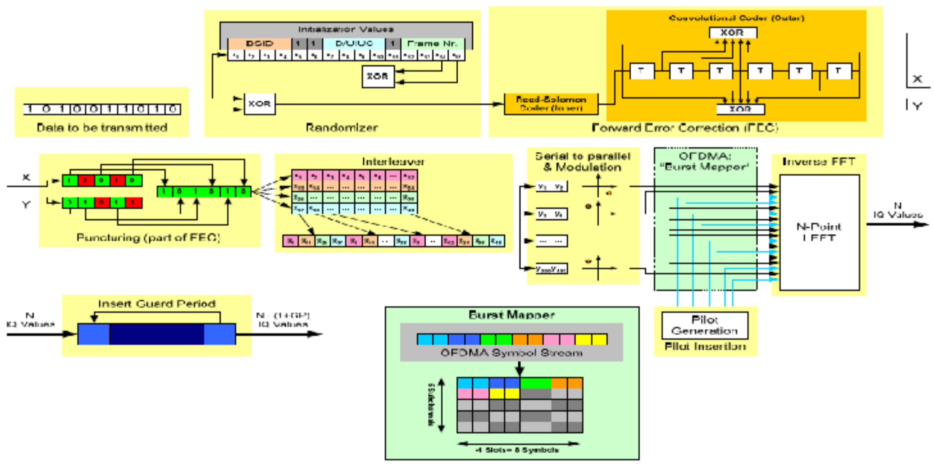


Fig.2.25: OFDM / OFDMA transmitter architecture (simplified)

After that, the Forward Error Correction (FEC) coder adds redundancy to the signal. This is a means of correcting errors that may occur during signal transmission. The coder is implemented as a *"Reed-Solomon coder"* as inner coding and a *"Convolution coder"* as outer coder. The total number of bits after encoding is higher than the number of bits before encoding.

Alternatively, "turbo coding" can be added as a block turbo coder or convolution turbo coder, which performs better but is also more complex.

The signal's number of bits must now be reduced. This is done within the *puncturing* device. It removes parts of the two output streams of the FEC and joins them in a defined way depending on the selected coding rate.

The *interleaver* now takes the bit stream and rearranges the data in a different order. This is done to protect against burst (or block) errors that can occur due to fading, signal level drops or other RF conditions.

The bit sequence leaving the interleaver is converted from serial to parallel (width depends on the FFT size) and applied to a modulator that performs a specific modulation scheme on the data (BPSK, 16QAM, etc).

For **OFDMA**, the data from one user occupies a certain amount of frequency and time resource. This mapping depends on different parameters such as amount of data to transmit, zone type, segment, subchannel group, etc.

A logical carrier can be built up from more than one physical carrier, which are normally nonadjacent physical carriers. This mapping is done by a burst mapper, which arranges the data in accordance with the rules defined in the standard.

All operations up to now lead to a complex-value and symbol-based representation of the data in frequency domain. This frequency domain data is now transformed to the time domain by means of an FFT block, which takes a certain number of *data carriers*, maps them to the FFT inputs (where the mapping rule may depend on complex rules) and adds a certain number of pilot carriers.

The pilot carriers are used to recover the absolute phase and phase response of the transmission channel, and allow the receiver to recover information about the transmission channel. The output data is now complex values in the time domain.

After the FFT block, the Guard Period is inserted into the IQ stream to overcome the problem of multipath effects on the **OFDM** signal, is then filtered by a baseband filter and passed to the D/A converter section, where it is converted to the transmission frequency and finally transmitted.

Protocol layers

Chapter 3

3.1 Protocol Model

The IEEE 802.16 protocol is a member of the IEEE 802 family of standards and addresses the media access and physical layers. The protocol reference model is shown in **Figure 3.1**.

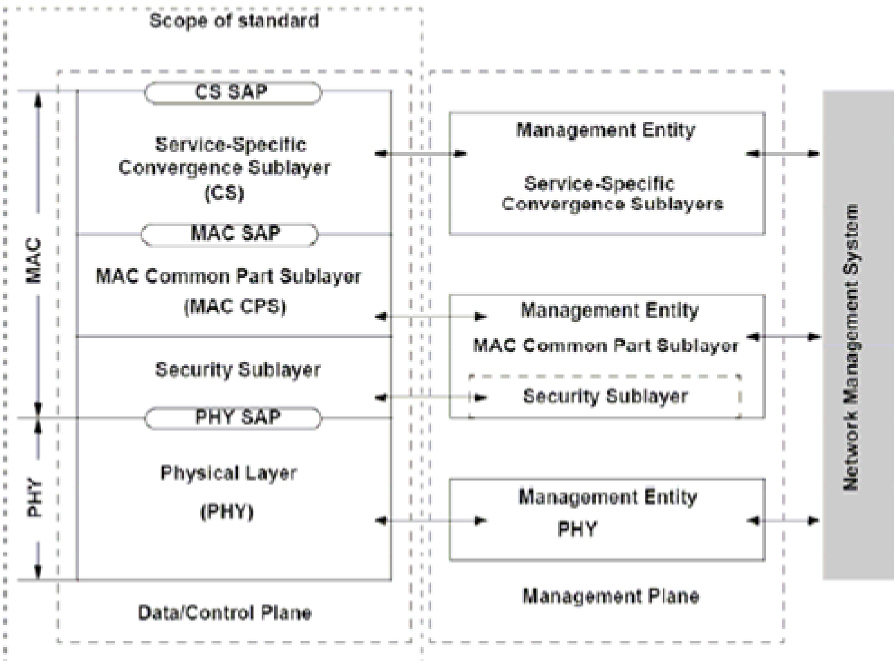


Fig.3.1: protocol reference model

A standard protocol-layering model is used. MAC peers communicate by sending/receiving data to/from the PHY layer. The PHY layers communicate via the 802.16 air link.

In the point-to-multipoint mode of operation, a base station transmits on the downlink channel to a collection subscriber stations by broadcasting the data to the stations that then select data that is addressed to them. Each

subscriber station communicates with a single base station and a collection of subscriber stations share an uplink channel for transmitting to the base via a multiple access scheme that is controlled by the base.

3.1.1 Physical Layer

In this section the supported access provision air interface technologies for different WiMAX profiles are elaborated.

3.1.1.1 OFDM

The WiMAX physical layer is based on Orthogonal Frequency Division Multiplexing. OFDM is the transmission scheme of choice to enable high-speed data communications in broadband systems. OFDM belongs to a family of transmission schemes called *multicarrier modulation*, which is based on the idea of dividing a given high-bit-rate data stream into several parallel lower bit-rate streams and modulating each stream on separate subcarriers. This technique helps us with minimizing the *Intersymbol Interference* (ISI). The number of substreams is chosen to ensure that each subchannel has a bandwidth less than the *coherence bandwidth* of the channel, so the subchannels experience relatively flat fading. In order to keep each OFDM symbol independent of the others after going through a wireless channel, it is necessary to introduce a *guard time* T_g, between OFDM symbols.

This way, after receiving a series of OFDM symbols with duration Ts, as long as the guard time is larger than the delay spread of the channel, each OFDM symbol will interfere only with itself. In order to completely eliminate the ISI and benefit a ISI-free channel *Cyclic Prefix* technique is used. **Figure 3.2** explains the concept of CP. The ratio of cyclic prefix to useful symbol time is indicated by *G* and can undertake values of 1/4, 1/8, 1/16 or 1/32.

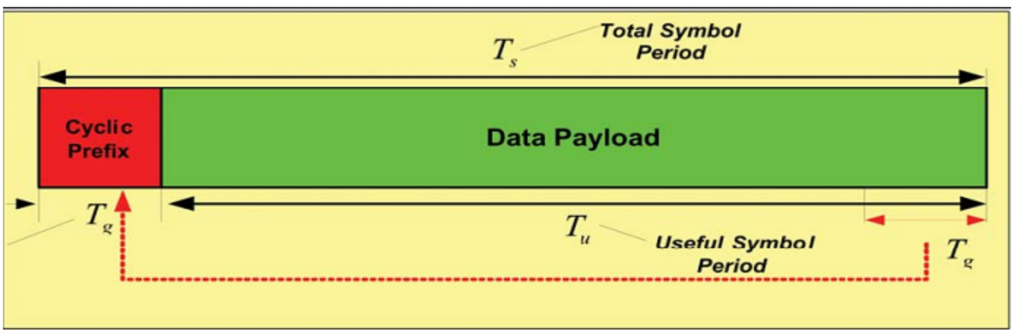


Fig.3.2: OFDM Symbol Structure with Cyclic Prefix

3.1.1.2 OFDMA

The total capacity available with a base station is shared among multiple users on a demand basis, using a burst TDM scheme. When using the OFDMA-PHY mode, multiplexing is additionally done in the frequency dimension, by allocating different subsets of OFDM subcarriers to different users. This is done based on subchannelization method.

Subchannelization is the method that differentiates OFDMA with OFDM. The available subcarriers within the total bandwidth can be divided into several groups of subcarriers called subchannels. Subchannels can be assigned to the users on a logical procedure based on user demands and channel conditions. OFDMA is essentially a hybrid of FDMA and TDMA: Users are dynamically assigned subcarriers (FDMA) in different time slots (TDMA).

There are 4 different types of subcarriers in an OFDMA symbol. *Data* subcarriers and *Pilot* subcarriers (used for estimation and synchronization purposes). These two first types are considered *Active subcarriers*. *DC* subcarriers together with *Guard* subcarriers (used for guard bands) are commonly denominated as *Null subcarriers*. **Figure 3.3** illustrates the OFDMA symbol's subcarrier structure.

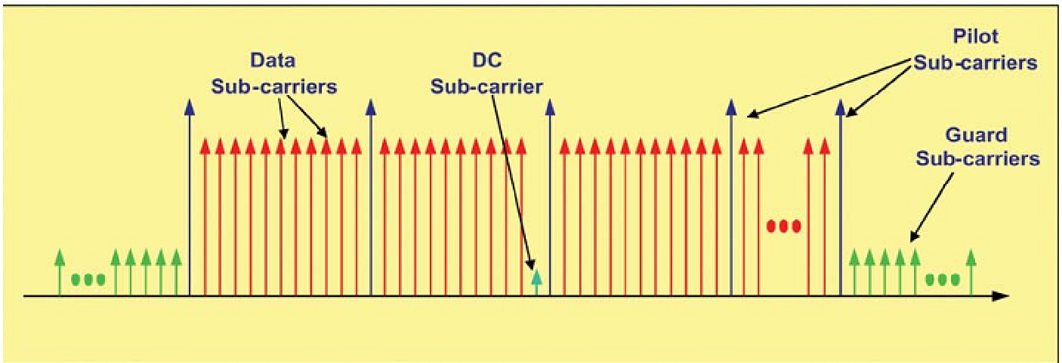


Fig.3.3: Frequency domain representation of OFDMA symbol

The number and exact distribution of the subcarriers that constitute a subchannel depend on the ***subcarrier permutation mode***. A *distributed* subcarrier permutation draws subcarriers pseudo-randomly to form a subchannel and provides better frequency diversity, whereas an *adjacent* subcarrier distribution allows the system to exploit multiuser diversity. In general, distributed (diversity) permutations perform well in mobile applications while adjacent (contiguous) permutations are well appropriated for fixed, portable or low mobility environments. In order for each MS to know which subcarriers are intended for it, the BS must broadcast this information in

downlink *MAP messages*. **Figure 3.4** reveals a graphical comparison between OFDM and OFDMA considering 4 different users sharing same bandwidth in both techniques in the uplink.

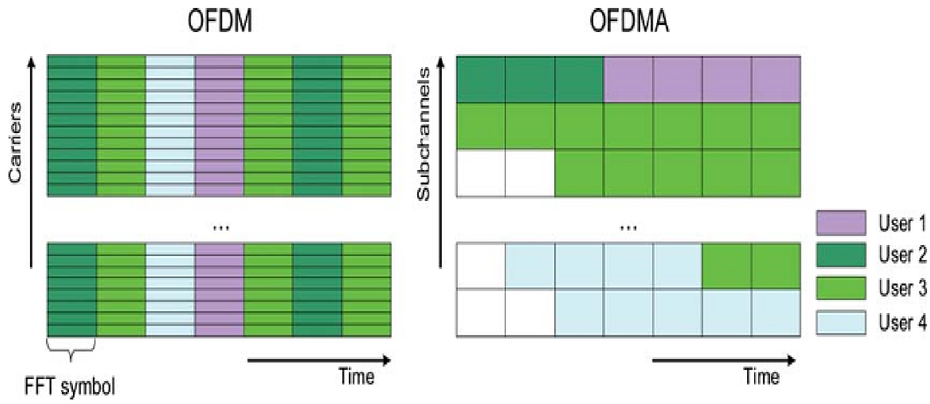


Fig.3.4: OFDM and OFDMA channel allocation in uplink

3.1.1.3 SOFDMA:

The mobile WiMAX - IEEE 802.16e-2005, is based on Scalable Orthogonal Frequency Division Multiple Access. The available bandwidth for WiMAX can vary based on the local frequency usage over the globe and the scalability is developed to support these worldwide variations. Therefore SOFDMA refers to the capability of choosing the number of subcarriers according to the available bandwidth. The channel bandwidth can vary from 1.25 MHz to 20 MHz and thus, a number of 128 to 2048 subcarriers can be assigned to each bandwidth correspondingly.

Table 3.1 summarizes the OFDM symbol parameters for Fixed WiMAX (IEEE 802.162004) and the equivalent OFDMA symbol parameters used in Mobile WiMAX (IEEE 802.16e-2005) in downlink direction. The diverse values for parameters in OFDMA refer to the scalability concept.

Table 3.1: *OFDM symbol parameters for Fixed WiMAX and the equivalent OFDMA symbol parameters used in Mobile WiMAX in downlink.*

Parameter	Fixed WiMAX OFDM-PHY	Mobile WiMAX Scalable OFDMA-PHY[a]			
FFT size	256	128	**512**	1,024	2,048
Number of used data subcarriers[b]	192	72	**360**	720	1,440
Number of pilot subcarriers	8	12	**60**	120	240
Number of null/guardband subcarriers	56	44	**92**	184	368
Cyclic prefix or guard time (Tg/Tb)	1/32, 1/16, **1/8**, 1/4				
Oversampling rate (Fs/BW)	Depends on bandwidth: 7/6 for 256 OFDM, 8/7 for multiples of 1.75MHz, and 28/25 for multiples of 1.25MHz, 1.5MHz, 2MHz, or 2.75MHz.				
Channel bandwidth (MHz)	3.5	1.25	**5**	10	20
Subcarrier frequency spacing (kHz)	15.625	**10.94**			
Useful symbol time (µs)	64	**91.4**			
Guard time assuming 12.5% (µs)	8	**11.4**			
OFDM symbol duration (µs)	72	**102.9**			
Number of OFDM symbols in 5 ms frame	69	**48.0**			

a. Boldfaced values correspond to those of the initial mobile WiMAX system profiles.

b. The mobile WiMAX subcarrier distribution listed is for downlink PUSC (partial usage of subcarrier).

As can be observed in **Table 3.1**, the subcarrier distribution for Mobile profile is derived with respect to ***PUSC permutation*** mode that is the mandatory resource grouping method in IEEE 802-16e standard. In this permutation mode, the DL usable sub-carriers (pilot and data) are grouped in clusters where each cluster contains *14* contiguous sub-carriers per symbol. Each cluster will be integrated by *12* data sub-carriers and *2* pilot subcarriers. So as an example in *5MHz* channel since we have *360* data sub-carriers and *60* pilot subcarriers, there will be *(360+60)/(12+2)=30* clusters. In addition, each subchannel is composed by 2 clusters, so there will be 30/2 = 15 subchannels in *DL PUSC*. The standard also defines *FUSC* (Fully Used Sub-Carriers) as an optional alternative permutation mode.

3.1.1.4 Channel Modulation and Coding

The mandatory coding scheme used in IEEE 802-16e is Convolutional Coding , CC. Several optional encoding methods such as turbo coding and low density parity check coding are also defined in the standard. Different coding rates of ½ and ¾ can be used within the coding stage with respect to DL and UL.

After encoding, the next step is interleaving. The encoded bits are interleaved using a two step process. The first step ensures that the adjacent coded bits are mapped onto nonadjacent subcarriers, which provides frequency diversity and improves the performance of the decoder. The second step ensures that adjacent bits are alternately mapped to less and more significant bits of the modulation constellation. During the *symbol mapping* stage, the sequence of binary bits is converted to a sequence of complex valued symbols. The mandatory constellations are QPSK and 16-QAM, with an optional 64-QAM constellation.

Higher modulation levels provide higher data rates. These tones are used to modulate the subcarriers and will form the subchannels based on the subcarrier permutation mode. The number of subchannels allocated for transmitting a data block depends on various parameters, such as the size of the data block, the modulation format, and the coding rate.

The overall information about the transmitted data will be presented in a *burst profile*. The burst profile provides the receiver with information like : modulation type, channel coding rate, coding and error correction schemes.

3.1.1.5 Frame Structure

In IEEE 802.16e-2005, both *frequency division duplexing* and *time division duplexing* are allowed. In the case of FDD, the uplink and downlink subframes are transmitted simultaneously on different carrier frequencies; in the case of TDD, the uplink and downlink subframes are transmitted on the same carrier frequency at different times. It should be noted that all the current candidate mobility profiles are TDD based. That is because of TDD's higher efficiency in asymmetric traffic: most of the times downlink occupies a higher ratio of the total frame. The TDD WiMAX frame is divided into 2 subframes for DL and

UL. These two subframes are separated with a transmission gap. **Figure 3.5** illustrates the TDD frame structure of WiMAX.

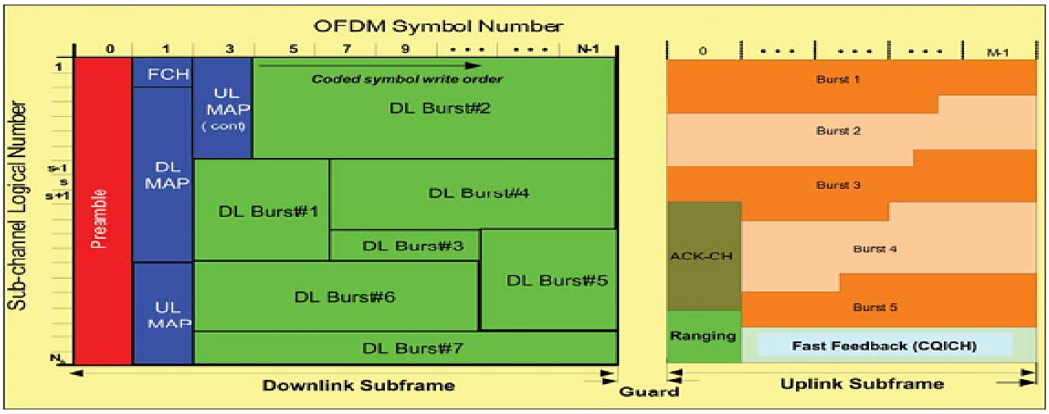


Fig.3.5: WiMAX OFDMA TDD Frame Structure

The first OFDM symbol in the downlink subframe is used for transmitting the *DL preamble* that is used for a variety of PHY layer procedures, such as time and frequency synchronization, initial channel estimation, and noise and interference estimation. *Frame Control Header (FCH)* specifies the some characters of the bursts such as length and number of the bursts. The *DL MAP* and *UL MAP* introduce the channel allocation information that are broadcasted to all users. Listening to MAP messages each user can identify the data region (sub-carriers) allocated for its use in both DL and UL. Each *DL data burst* is assigned a burst profile and contains the data for an individual user.

The *ranging* in the uplink is done to assure a reliable communication by performing time and power synchronization. Bandwidth request with the users may be followed by ranging symbols. Then the users transmit in each UL data Burst within their allocated subcarriers, already known by UL MAP. The *Uplink Channel Quality Indicator* (CQICH) is allocated to feedback channel state of each terminal to the BS's scheduler to be used for AMC as an example. The *ACK* uplink channel is the downlink HARQ acknowledgment.

Since the OFDMA PHY layer has many choices of subcarrier allocation methods, multiple zones can use different subcarrier allocation methods to divide each subframe. One benefit of using zone switching is that different frequency *reuse factors (FRF)* can be deployed in a cell or sector, dynamically. **Figure 3.6** shows an example of deploying different FRFs in one frame. For the first half of each frame, the entire frequency band is divided by three and allocated in each sector. For the second half of each frame, the whole same

frequency band is used in each sector. The benefits of deploying different FRFs in one frame are:

- The FCH and DL-MAP are highly protected from severe cochannel interference;
- Edge users, who are receiving co-channel interference from other sectors in other cells, also have suppressed co-channel interference;
- Users around the cell center have the full frequency band because they are relatively less subject to co-channel interference.

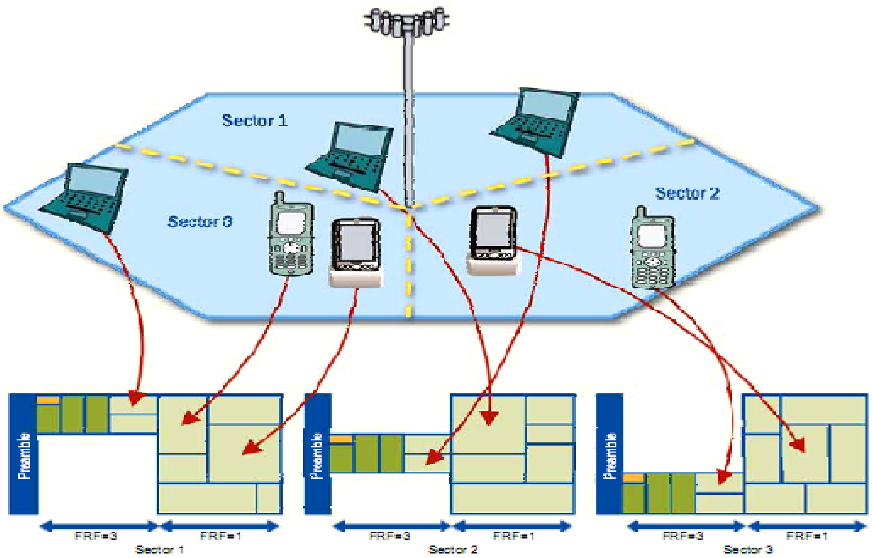


Fig.3.6: Frequency Reuse Implementation in Sectoring

3.1.2 MAC Layer

In WiMAX technology, second network layer plays some critical roles in the specification such as packeting and fragmentation, channel allocation, scheduling, QOS and security provision and finally mobility management. In this section the MAC layer's entity and tasks are mentioned.

3.1.2.1 MAC Layer Structure

The WiMAX MAC layer consists of 3 sublayers as it is revealed in **Figure 3.7**.

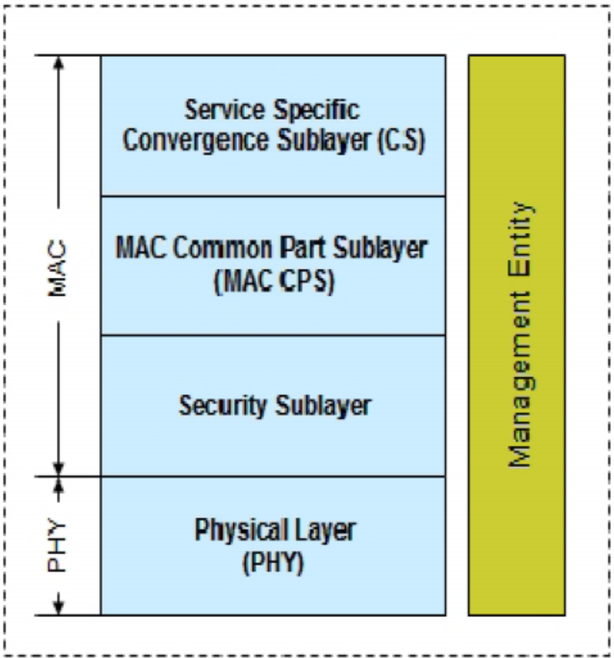


Fig.3.7: WiMAX MAC layer

- **The *Convergence Sublayer*,** CS, that treats as the interface between any higher layers above MAC layer and its lower sublayers. CS receives higher layer packets also known as *Service Data Units, SDU*, and maps them into appropriate forms for further processes within MAC layer, such packet address identifications. Whereas both ATM and IP connotations are defined in the IEEE 802.16e standard, WiMAX Forum has decided to implement only IP services.

- ***MAC common part sublayer*** is responsible for receiving SDUs and applying appropriate fragmentation and concatenation over them , forming MAC *PDUs* , *Protocol Data Units,* and preparing PDUs for transmission. Based on the size of the payload, multiple SDUs can be carried on a single MAC PDU, or a single SDU can be fragmented to be carried over multiple MAC PDUs. Quality of service, *QOS,* control channel allocation and scheduling are other tasks made in this sublayer.

- ***MAC Security Sublayer***, as the name implies, handles security tasks such as authentication and encryption.

3.1.2.2 MAC PDU Structure

Each MAC PDU (protocol data unit) consists of a header followed by a payload and a cyclic redundancy check, CRC, as can be seen in **Figure 3.8.** There are two types of MAC PDUs :

- ***The generic MAC PDU*** is used for carrying data and MAC-layer signaling messages. A generic MAC PDU starts with a generic header consisted of 6 bytes and followed by payload and CRC.

- **The bandwidth request PDU** consisted only of a bandwidth request header, with no payload or CRC. The Generic Header may contain other subheaders for different purposes.

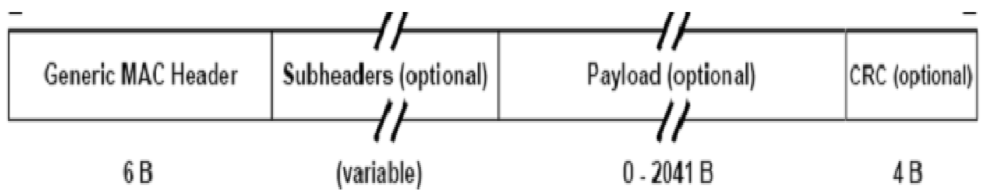


Fig.3.8: MAC PDU Structure

Once a MAC PDU is constructed, it is handed over to the *scheduler*, which schedules the MAC PDU over the PHY resources available. The scheduler determines the optimum PHY resource allocation for all the MAC PDUs, on a frame-by-frame basis. Based on the traffic class, the scheduler can assign the whole frame or a single time slot to a terminal. It is good to note that WiMAX is designed to support all different traffic modules out of 4 different existing ones. These are: Background (messages), Interactive (web browsing), Streaming (video) and Conversational (VoIP) in delay sensitivity increasing order.

3.1.2.3 Bandwidth Allocation

In the downlink, all decisions related to the allocation of bandwidth to various MSs are made by the BS without the involvement of the MS based on CID, Connection Identifier. These CIDs are 16-bit addresses used to distinguish between multiple UL channels (connections) associated with the same DL channel. The Mobile Stations or Subscriber Stations, SS, check CIDs in the received PDUs and retain only those PDUs that are addressed to them.

As mentioned before, the PHY recourses allocated for PDU transmission in each connection is indicated in DL-MAP messages.

In the uplink, the MS requests resources by using a bandwidth request subheader on a MAC PDU. The BS allocates dedicated (intended for a single SS) or shared (intended for a group of SSs) resources for the users periodically which can be used to request bandwidth. In WiMAX this process is called Polling.

3.1.2.4 Quality of Service (QOS) and Scheduling

Each user can achieve the desired bandwidth based on the Quality of service that is defined for it. The system should grant a reliable connection based on the agreed QOS parameters within a connection. A key concept in QOS is *Service Flow.* Each service flow or category is associated with a unique set of QOS parameters, such as latency, jitter throughput, and packet error rate, that the system strives to offer. **Table 3.2** illustrates service flows supported in Mobile WiMAX and gives example applications for each. Before providing any certain type data service, the BS's MAC establishes an unidirectional connection with its peer MAC layer in the user terminal to discuss the agreed service flow and assign the QOS parameters over the air interface.

The efficiency of resource allocation (time and frequency) in both DL and UL is controlled by the *scheduler* that is located in each BS. The scheduler controls the traffic trend by monitoring CQICH feedback to provide the best resource allocation that supports the QOS parameters for each connection. The scheduling process is done on a frame by frame base in response to traffic and channel conditions.

Table 3.2: *Mobile WiMAX Service Flows and QOS parameters*

QoS Category	Applications	QoS Specifications
UGS Unsolicited Grant Service	VoIP	• Maximum Sustained Rate • Maximum Latency Tolerance • Jitter Tolerance
rtPS Real-Time Polling Service	Streaming Audio or Video	• Minimum Reserved Rate • Maximum Sustained Rate • Maximum Latency Tolerance • Traffic Priority
ErtPS Extended Real-Time Polling Service	Voice with Activity Detection (VoIP)	• Minimum Reserved Rate • Maximum Sustained Rate • Maximum Latency Tolerance • Jitter Tolerance • Traffic Priority
nrtPS Non-Real-Time Polling Service	File Transfer Protocol (FTP)	• Minimum Reserved Rate • Maximum Sustained Rate • Traffic Priority
BE Best-Effort Service	Data Transfer, Web Browsing, etc.	• Maximum Sustained Rate • Traffic Priority

3.1.2.5 Mobility Management

The mobile WiMAX standard IEEE 802.16e introduces several new concepts related to mobility management and power management, two of the most fundamental requirements of a mobile wireless network. Power management enables the MS to conserve its battery resources, a critical feature required for handheld devices. Mobility management, on the other hand, enables the MS to retain its connectivity to the network while moving from the coverage area of one BS to the next. The last concept is also referred to as handoff.

3.1.2.5.1 Power Control

The power control is made of two major modes: Sleep Mode in which the Mobile station with active connections negotiates with the BS to temporarily disrupt its connection over the air interface for a predetermined amount of time, called the sleep window. Each sleep window is followed by listen window, during which the MS restores its connection. The length of each sleep and listen window is negotiated between the MS and the BS and is dependent on the power saving class of the sleep-mode operation. During the unavailability interval (sleep mode), the BS does not schedule any DL transmissions to the MS, so that it can power down one or more hardware components required for communication. Within the sleep mode the BS performs the procedures needed for handoff (explained below) ,while in Idle Mode MS can eliminate these handoff procedure hardwares causing more power consumption. However during Idle mode the BSs performs paging to update the new location of the MS.

3.1.2.5.2 Handoff

The IEEE 802.16e Standard defines signaling mechanisms for tracking Subscriber Stations as they move from the coverage range of one base station to another when active mode or as they move from one paging group to another when idle mode. The BS allocates time for each MS to monitor the radio condition of the neighboring BSs by measuring the received signal strength indicator (RSSI) of the BSs located within the active set of base stations. This process is called *scanning.* The MS can associate with some other BSs while it is connected to an individual one. The handoff process begins with the decision for the MS to migrate its connections from the serving BS to a new target BS. This decision can be taken by the MS, the BS, or some other external entity in the WiMAX network and is dependent on the implementation. Once a handover decision is made, the MS begins synchronization with the DL transmission of the objective BS listening to its preamble, performs ranging if

it has not been realized while scanning, and then terminates the connection with the previous BS. The explained method is known as *Hard Handoff, HHO*, method which is the only mandatory handoff defined for WiMAX certified products. In HHO an abrupt exchange of connection from one BS to another is done. However there are other methods such as Fast Base Station Switching (FBSS) and Macro Diversity Handover (MDHO) which in both methods, the MS maintains a valid connection at the same time with more than one BS.

Chapter 4

Physical layer WiMAX
T_X &R_X

4.1 Introduction

The physical (PHY) layer of WiMAX is based on the IEEE 802.16-2004 and IEEE 802.16e2005 standards and was designed with much influence from Wi-Fi, especially IEEE802.11a. Although many aspects of the two technologies are different due to the inherent difference in their purpose and applications, some of their basic constructs are very similar. Like Wi-Fi, WiMAX is based on the principles of orthogonal frequency division multiplexing (OFDM), which is a suitable modulation/access technique for non line of sight (NLOS) conditions with high data rates. In WiMAX, however, the various parameters pertaining to the physical layer, such as number of subcarriers, pilots, guard band and so on, are quite different from Wi-Fi, since the two technologies are expected to function in very different environments. The IEEE 802.16 suite of standards (IEEE 802.16-2004/IEEE 802-16e-2005) defines within its scope four PHY layers, any of which can be used with the media access control (MAC) layer to develop a broadband wireless system.
The PHY layers defined in IEEE 802.16 are

• ***Wireless MAN SC,*** a single-carrier PHY layer intended for frequencies beyond 11GHz requiring a LOS condition. This PHY layer is part of the original 802.16 specifications.

• ***Wireless MAN SCa,*** a single-carrier PHY for frequencies between 2GHz and 11GHz for point-to-multipoint operations.

• ***Wireless MAN OFDM,*** a 256-point FFT-based OFDM PHY layer for point-to-multipoint operations in non-LOS conditions at frequencies between 2GHz and 11GHz. This PHY layer, finalized in the IEEE 802.16-2004 specifications, has been accepted by WiMAX for fixed operations and is often referred to as fixed WiMAX.

• ***Wireless MAN OFDMA,*** a 2048-point FFT-based OFDMA PHY for point-to-multipoint operations in NLOS conditions at frequencies between 2GHz and 11GHz. In the IEEE 802.16e-2005 specifications, this PHY layer has been modified to SOFDMA (scalable OFDMA), where the FFT size is variable and can take any one of the following values: 128, 512, 1024, and 2048. The variable FFT size allows for optimum operation/implementation of the system over a wide range of channel bandwidths and radio conditions. This PHY layer has been accepted by WiMAX for mobile and portable operations and is also referred to as mobile WiMAX.

4.2 WiMAX Transmitter

The functional blocks which compose the WiMAX transmitter are shown in figure 2.1. The MAC Payload Data Units (PDUs) are fed into the randomizer which randomizes the data. Afterwards, the randomized data is coded by using channel encoder as, which consists of Reed Solomon, convolutional encoder and puncture. The coded data is interleaved by interleaver and mapped into QAM symbol. Afterwards, the mapped data enter into the OFDM modulation which consist of assemble OFDM frame, 256 IFFT and cyclic prefix insertion. Then the data is transmitted over AWGN channel. Through the rest of chapter the individual block of the WiMAX transmitter will be explained.

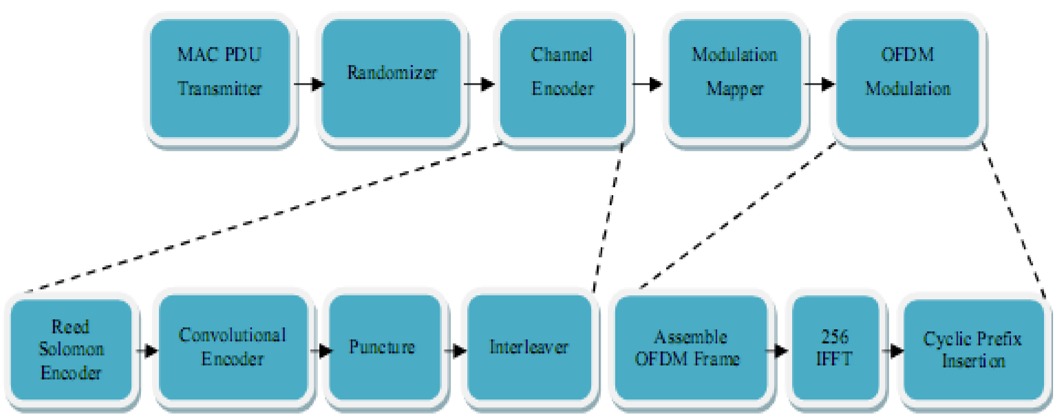


Fig.4.1: *The mandatory parts of WiMAX Transmitter*

4.2.1 Randomizer

The information bits are randomized before the transmission. The randomizer, which is the first block in the transmitter, performs randomization

of input data on each burst on each allocation to prevent a long sequence of 1's and 0's. This is implemented by using a Pseudo Random Binary Sequence (PRBS) generator, which is made of a 15 bits shift register and two XOR gates as shown in **Figure 4.2**.

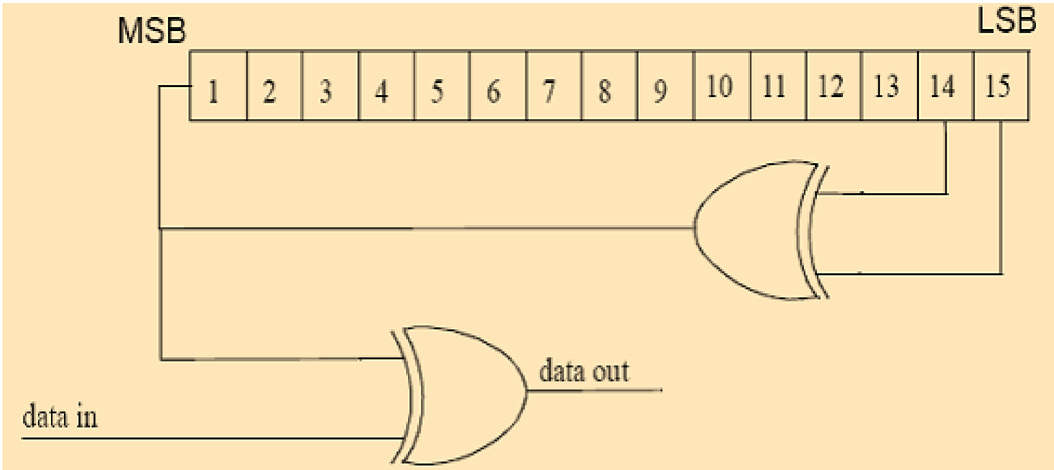


Fig.4.2: Point PRBS for data randomization

For downlink burst the initial vector for the shift register (Linear-Feedback Shift Register (LFSR) possessing characteristic polynomial $1 + x^{14} + x^{15}$ is 100101010000000 and the scrambler should be reset at the start of each burst. The vector, which is shown in **Figure 4.3**, is placed at the start of subsequent bursts. We utilize frame number for referring to the frame in which the downlink burst is transmitted.

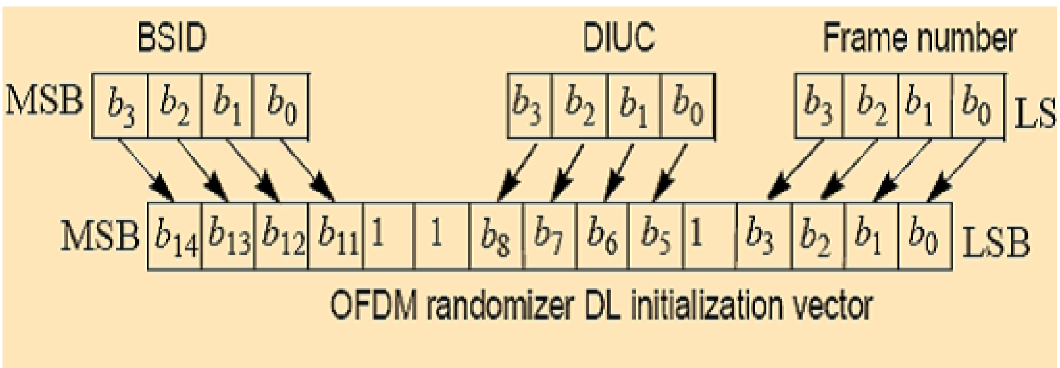


Fig.4.3: OFDM randomizer downlink initialization vector for burst #2...N

4.2.2 Channel Encoder

The channel encoder consists of an FEC scheme (i.e. a concatenation of an outer RS code and an inner CC), puncturing and interleaving as shown in **Figure 4.1**. The randomized data passes to the RS encoder and then passes to CC encoder. After this, the encoded data is punctured and interleaved.

4.2.2.1 Outer Reed Solomon Encoder

The RS code is special kind of linear block codes, which is suitable for correcting burst errors. The RS encoder adds redundancy to the data sequence in order to correct the errors, which occurred during transmission. This RS code is derived from a systematic RS **(N = 255, K = 239,T =8)** code using a Galois field specified as GI $\mathbf{2^8}$, with N is the number of bytes after encoding, K is the number of data bytes before encoding and T is the number of data byte that can be corrected.

The following polynomials are used for the systematic code:

Code Generator Polynomial:

$$g(x) = (x + y^0) + (x + y^1) + (x + y^2) \cdots\cdots (x + y^{2T-1})$$

Field Generator Polynomial:

$$p(x) = x^8 + x^4 + x^3 + x^2 + 1$$

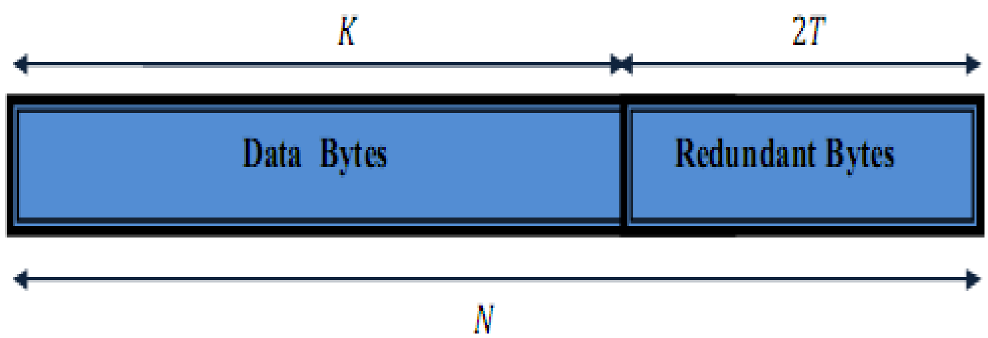


Fig.4.4: The Reed Solomon code

In WiMAX RS code is shortened and punctured to enable variable block sizes and variable error-correction capability. We can obtain a shortened block of bytes by adding **239 −K′** zero bytes before the data block, these **239 −K′** zero bytes are discarded after encoding. RS code can correct up to **T** symbols, where **T** can be expressed as **T = (N−K)/2**. When a codeword is punctured to permit T' bytes to be corrected. Only the first **2** T' of the total **16** parity bytes shall be employed as shown in **Figure 4.5**. For instance, QPSK with **(5/6)** CC code rate, the RS code is ($(N' = 40)$,$(K' = 36)$, $(T' = 2)$) as shown in **Table 4.1**. The bit/byte conversion has to be MSB first.

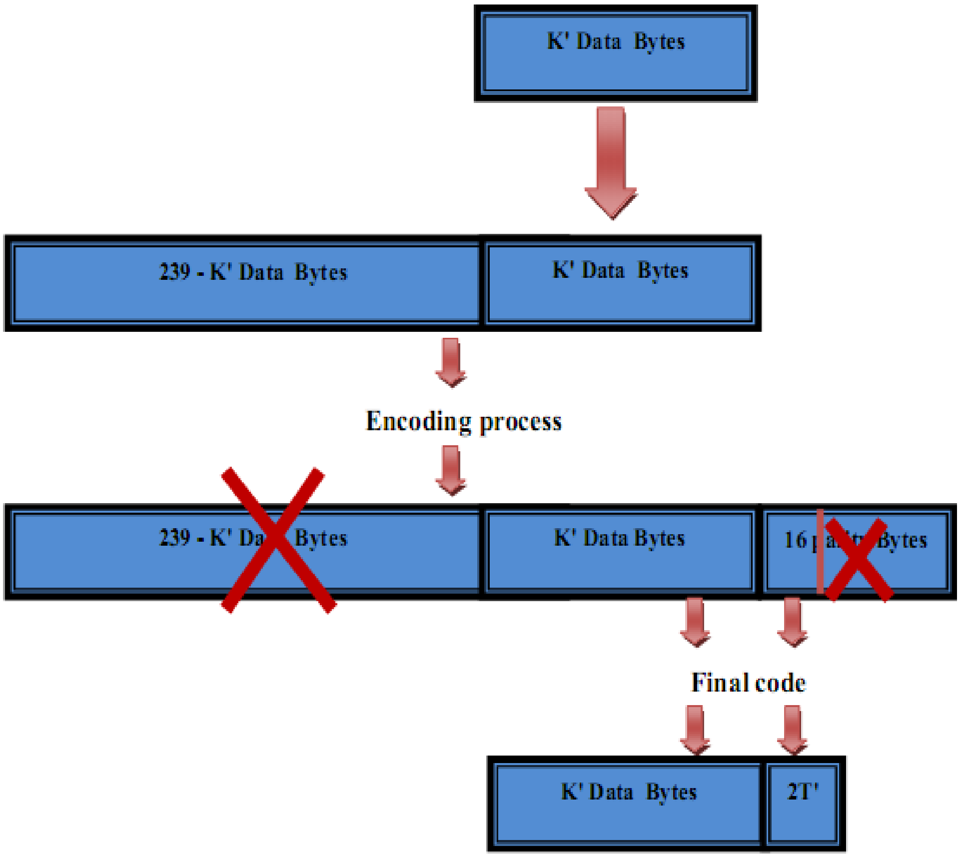


Fig.4.5: Shortening and puncturing process of the RS code

4.2.2.2 Inner Convolutional Encoder

The random errors which occurred during the transmission over channel can be corrected by using the convolutional encoder. Unlike a block coder, convolutional coder is not a memory less device. The RS encoded bits are encoded by the binary convolutional encoder, which has native rate of **1/2**, a constraint length equal to **7** and a polynomial description **[171 133]** to produce its two code bits. The generator is shown in figure 2.6.

$$G_1 = 171_{OCT} \qquad for\ X$$

$$G_1 = 133_{OCT} \qquad for\ Y$$

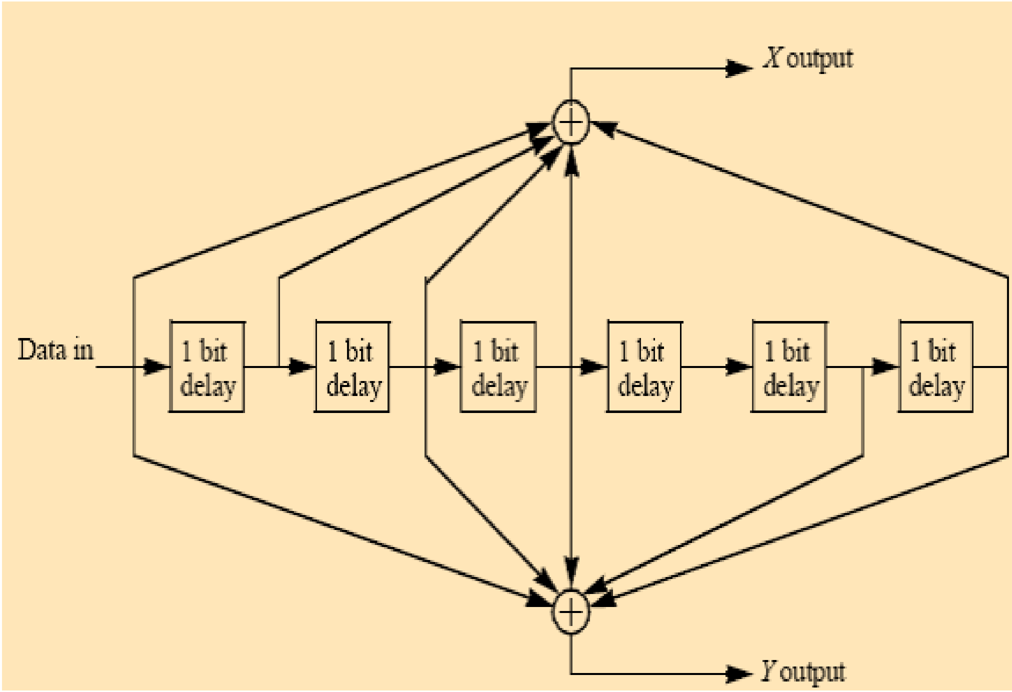


Fig.4.6: *Convolutional encoder of rate 1/2*

In WiMAX, after the randomized data is encoded by RS encoder, the encoded bits are forwarded to convolutional encoder. The block sizes and the code rates, which are used for the different types of modulation and code rates, are given in **Table 4.1**.

Table 4.1: *Mandatory channel coding per modulation*

Modulation	Uncoded block size (bytes)	Coded block size (bytes)	Overall coding rate	RS code	CC code rate
BPSK	12	24	1/2	(12,12,0)	1/2
QPSK	24	48	1/2	(32,24,4)	2/3
QPSK	36	48	3/4	(40,36,2)	5/6
16-QAM	48	96	1/2	(64,48,8)	2/3
16-QAM	72	96	3/4	(80,72,4)	5/6
64-QAM	96	144	2/3	(108,96,6)	3/4
64-QAM	108	144	3/4	(120,108,6)	5/6

4. 2.2.3 Puncturing

Puncturing is a technique that is utilized on the output of the convolutional encoder. It allows the encoding and decoding of higher code rates using standard rate **1/2** encoders and decoders. The purpose of using puncturing is to achieve variable code rate. This is done by deleting bits from the output stream of a low rate encoder. The bits are deleted according to the **Table 4.2**. In this table, **"1"** means a transmitted bit and **"0"** denotes a removed bit, whereas and are in reference to figure 2.6.

Table 4.2: The inner convolutional code with puncturing configuration

	Code rates			
Rate	1/2	2/3	3/4	5/6
d_{free}	10	6	5	4
X	1	10	101	10101
Y	1	11	110	11010
XY	X_1Y_1	$X_1Y_1Y_2$	$X_1Y_1Y_2X_3$	$X_1Y_1Y_2X_3Y_4X_5$

4.2.2.4 Interleaver

The interleaver is the final part of channel encoder used to randomize the coded bits in order to make the possible errors at the receiver uncorrelated. All encoded bits coming from RS-CC encoder are interleaved by a block interleaver with a block size, which depends on the number of coded bits per allocated subchannels per OFDM symbol($\mathbf{N_{cbps}}$). The number of coded bits depends on modulation scheme as shown in **Table 4.3**. The interleaver in WiMAX is defined by a two step permutation. The first permutation ensures that adjacent coded bits are mapped onto non adjacent carriers.

$$m_k = (N_{cbps}/12) \,.\, k_{mod12} + floor(k/2)$$

The second permutation ensures that adjacent coded bits are mapped alternately onto less or more significant bits of the constellation.

$$j_k = s.\,floor(m_k/s) + (m_{k+}N_{cbps} - floor(12.\,m_k/N_{cbps}))_{mods}$$

With **s=ceil** $(\mathbf{N_{cpc}}/\mathbf{2})$, and $\mathbf{N_{cpc}}$ is the number of coded bit per carrier, $\mathbf{N_{cbps}}$ is number of coded bits per OFDM symbol, **k** is index of coded bits before first permutation, $\mathbf{m_k}$ is index of coded bits after first permutation and before the second permutation and $\mathbf{j_k}$ is index of coded bits after second permutation.

Table 4.3: *Block sizes of the bit interleaver*

	Default (16 subchannels)	8 subchannels	4 subchannels	2 subchannels	1 subchannel
	N_{cbps}				
BPSK	192	96	48	24	12
QPSK	384	192	96	48	24
16-QAM	768	384	192	96	48
64-QAM	1152	576	288	144	72

4.2.3 Modulation Mapper

In the modulation mapper, the interleaved bits are converted to a sequence of complex valued symbols. WiMAX supports different modulation schemes shown in figure 2.7. The modulation constellation used in WiMAX is two types of phase shift keying **(PSK)** modulation (*binary* **(BPSK)** *and quadrature* (QPSK)) and two types of quadrature amplitude **(QAM)** modulation **(16QAM** and **64QAM)**.The complex constellation value is scaled by factor (*Normalization constant*), such that the average transmitted power is unity, *c* equals $\mathbf{1/\sqrt{2}}$ for **QPSK**, $\mathbf{1/\sqrt{10}}$ for **16-QAM**, $\mathbf{1/\sqrt{42}}$ for **64-QAM** (*if we assume that all symbols are equally likely).*

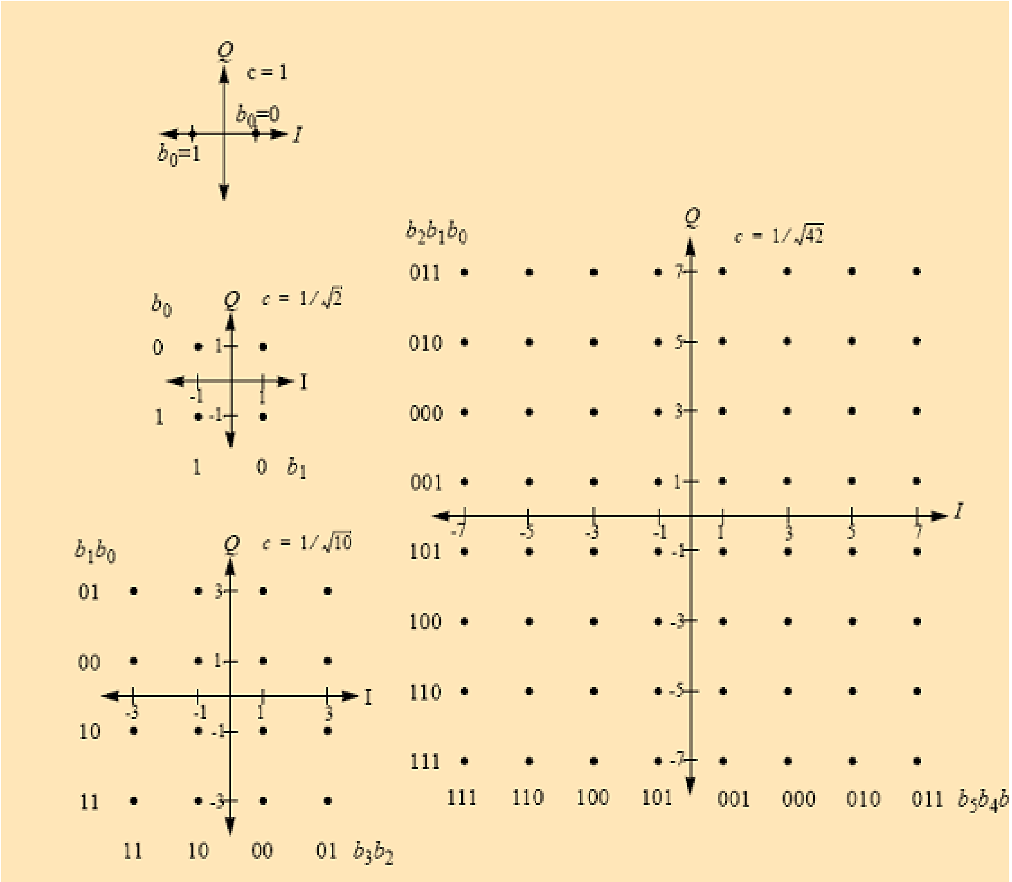


Fig.4.7: BPSK, QPSK, 16-QAM and 64-QAM constellations

4.2.4 OFDM modulation

In WiMAX, each OFDM symbol consists of 256 subcarriers as shown in **Figure 4.8**. They can be divided into.

- 192 data subcarriers that are used for conveying data.
- 8 pilot subcarriers that are used for conveying pilot symbols. 56 null subcarriers that have no power allocated to them, including the DC subcarrier and the guard subcarriers toward the edge.

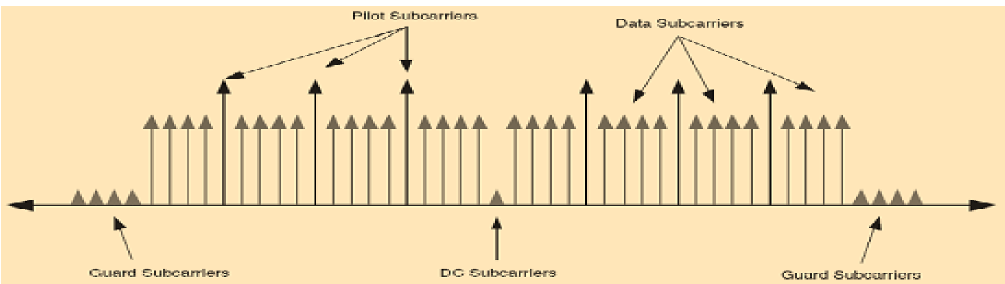


Fig.4.8: Frequency domain representation of OFDM symbol

4.2.4.1 Pilot modulation

Before inserting a pilot to its specified position, as shown in figure 2.8, it has to be modulated. Pilots can be generated by Pseudo Random Binary Sequence (PRBS) generator as shown in **Figure 4.9**.

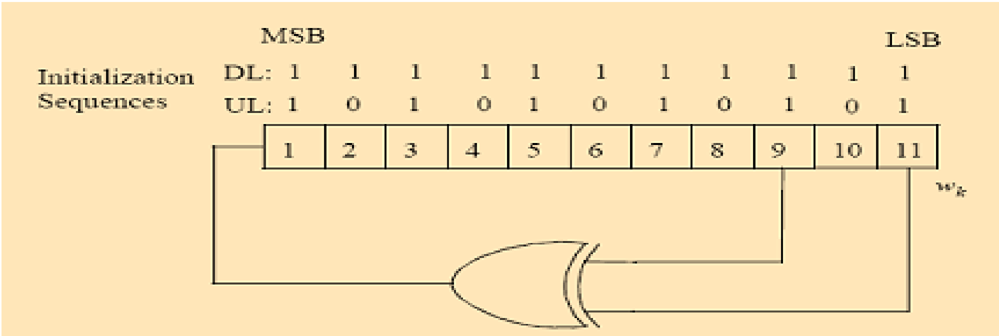


Fig.4.9: *PRBS for pilot modulation*

The polynomial of PRBS generator is:

$$g(x) = x^{11} + x^9 + 1$$

Pilot subcarriers are used for various estimation purposes.

4.2.4.2 Inverse Fast Fourier Transform (IFFT)

To convert mapped data, which is assigned to all allocated data subcarriers of the OFDM symbol, from frequency domain into time domain, the IFFT is used. We can compute time duration of the IFFT time signal by multiply the number of FFT bins by the sample period. Zeros are added at the end and beginning of OFDM symbol. These zero carriers are used as guard band to prevent inter channel interference **(ICI)**.

4.2.4.3 Cyclic Prefix insertion (CP)

To avoid inter symbol interference **(ISI)** a cyclic prefix is inserted before each transmitted symbol. That is achieved by copying the last part of an OFDM symbol to the beginning as shown in **Figure 4.10**. WiMAX supports four different duration of cyclic prefix (*i.e. assuming is the ratio of guard time to OFDM symbol time; this ratio is equal to* ***1/32****,* ***1/6****,* ***1/8*** *and* ***1/4****).*

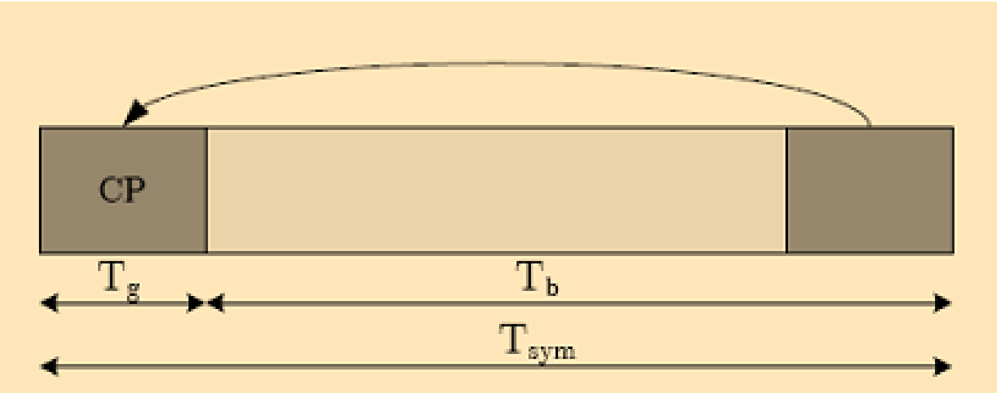


Fig.4.10: OFDM symbol with the cyclic prefix

4.3 WiMAX Receiver

This chapter describes the mandatory parts of WiMAX receiver. The functional blocks which compose the WiMAX receiver as shown in **Figure 4.11** are the reverse functional blocks of WiMAX transmitter. The received data coming from AWGN channel is fed into the OFDM demodulation, which consist of removal of CP, Fast Fourier Transform (256 FFT) and disassemble OFDM frame. Then, the data is performed by de-mapper and afterwards the demapped data enter the channel decoder. Channel decoder consists of de-interleaver, depuncture, convolutional decoder and finally RS decoder. The final block in receiver is the derandomizer. Through the rest of chapter the individual block of the WiMAX receiver will be explained.

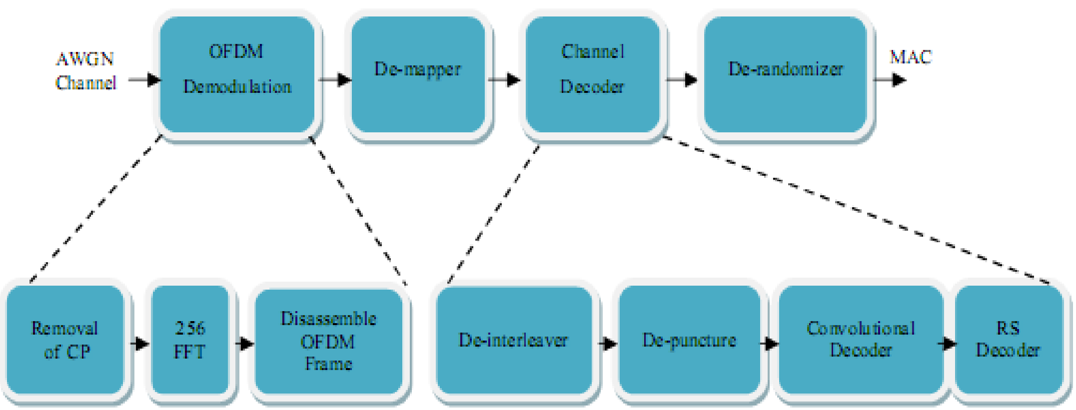


Fig.4.11: The mandatory parts of WiMAX Receiver

4.3.1 OFDM Demodulation

The OFDM demodulation is the reverse operation of OFDM modulation. Here, the signal is converted back from time domain to frequency domain. The first step in OFDM demodulation is to remove the CP. Then FFT is performed. Afterwards the OFDM frame is disassembled.

4.3.1.1 Removal of CP

The first step after the arrival of data is to remove CP as shown in **Figure 4.12**. We know that CP has no effect in case of using AWGN channel. It is useful when the multipath channel is used. If CP larger than the delay multipath the ISI is completely removed.

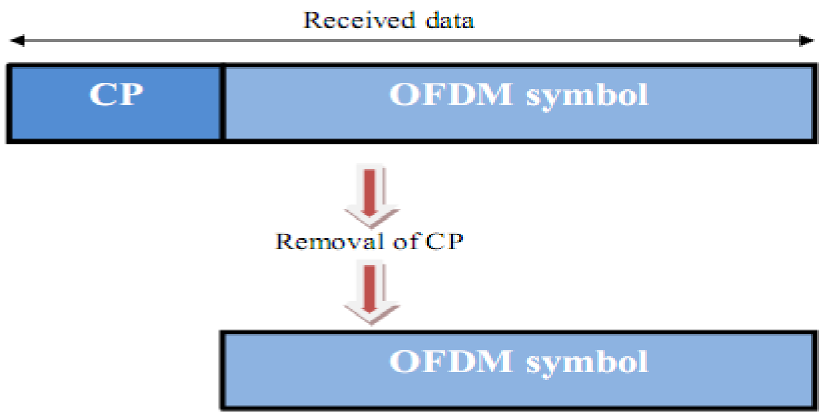


Fig.4.12: *Removal of CP*

4.3.1.2 Fast Fourier Transform (FFT)

To convert received data from time domain to frequency domain, the FFT is used. Afterward, the zeros, which were added at the end and beginning of OFDM symbol (guard bands) at the transmitter are removed from the assigned places.

4.3.1.3 Disassemble OFDM Frame

After doing FFT and removing guard bands, the data and pilots, which is described in **section 4.4** should be separated. This is achieved by using the disassembler.

4.3.2 Demapping

To convert the waveforms created at the modulation mapper to the original transformed bits, the de-mapper is used. The demapping is used for decision rules with the goal of making a decision about which bit "zero" or "one", was sent. The decision metric can be hard decision or soft decision. The minimum distance rule is the optimum decision in case of independent and identical distributed Gaussian noise.

4.3.3 Channel Decoder

The channel decoder consists of deinterleaving, depuncturing, Viterbi decoder and RS decoder as shown in figure 3.1. The sequence of bits coming from de-mapper passes to channel decoder. The channel decoder tries to recover the original bits.

4.3.4 Deinterleaving

To remove the effect of interleaving process achieved at the transmitter, the deinterleaving is used. Deinterleaver in WiMAX is defined by two-step permutation.

The first permutation is defined by equation:

$$m_j = s.floor(j/s) + (j + floor(12.j/N_{cbps}))_{mod(s)}$$

$$j = 0,1,\cdots,N_{cbps} - 1$$

The second permutation is defined by equation:

$$k_j = 12.m_{j\_}(N_{cbps} - 1).floor(12.m_j/N_{cbps})_{mod(s)}$$

$$j = 0,1,\cdots,N_{cbps} - 1$$

With **s=ceil ($N_{cpc}/2$)** , and $\mathbf{N_{cpc}}$ is the number of coded bit per carrier, $\mathbf{N_{cbps}}$ is number of coded bits per OFDM symbol (received block), **j** is the index of a received bit before the first permutation, $\mathbf{m_j}$ is the index of that bit after the first and before the second permutation and $\mathbf{k_j}$ is the index of

that bit after the second permutation. The number of coded bits depends on modulation scheme as shown in table 2.3.

4.3.5 Depuncturing

Depuncturing the reverse process of puncturing. Puncturing is done by deleting bits from certain places which was explained in table 2.2. At receiver, the values of deleted bits are unknown, so the receiver adds zeros in those places, which are known for. These inserted zeros can be seen as erasures from the channel. They have no effect on the metric measurement of the Viterbi algorithm.

4.3.6 Convolutional decoder

To decode the bit stream coming after depuncturing, the convolutional decoder is used. The Viterbi algorithm is the one of methods, which is commonly used for decoding the convolutional codes. The Viterbi algorithm performs the maximum likelihood decoding. It is described by using the trellis diagrams as shown in **Figure 4.13**. The algorithm computes the distance between the received sequence at certain time and each trellis paths entering each state at the same time. When two paths met in single state, the algorithm chooses the one, whose better metric (i.e. smaller Hamming distance). And so on, till remain a single path which represents the received data (the surviving path). Comparing the received sequence with every possible code sequence is the best way to detect the random errors.

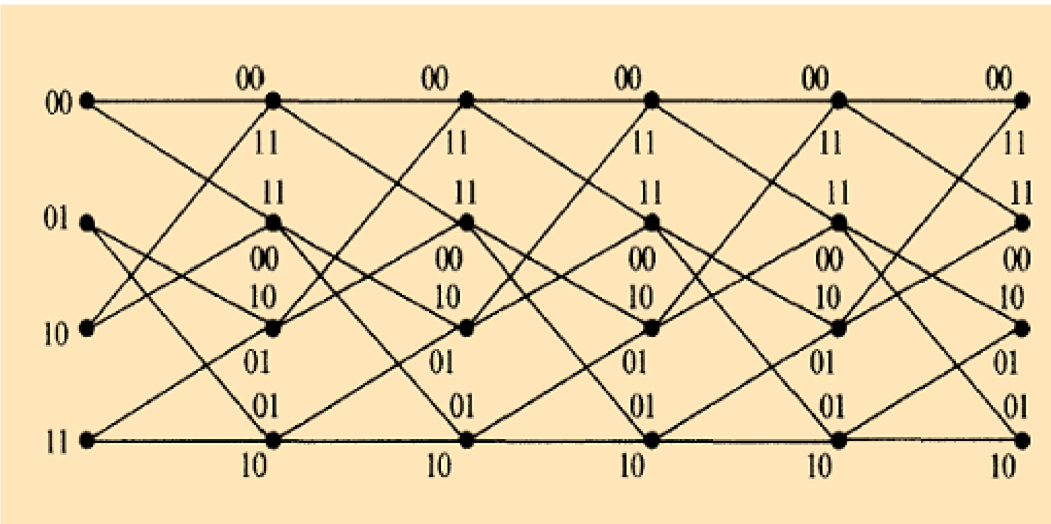


Fig.4.13: *The trellis diagram*

4.3.7 Reed Solomon Decoder

The RS decoder is the last part in channel decoder. The operation of RS decoder is the reverse operation of RS encoder. we know that the output data block of RS encoder was $(K' + 2T')$ as shown in **Figure 4.4**. So, to make the output of convolutional decoder entering to the RS decoder as the same. The one that output the encoder block, the first step is this output is reshaped. That means, each 8 bits is converted to byte and rearranged it according to the table 3.1. For instance, **QPSK** with **(5/6)** CC code rate, the RS code is **((N'=40), (K'=36), (T'=2))**. Afterwards the **239 –K'** zero bytes is added at the beginning of each block. And the **16 – 2T'** parity bytes are obtained by add zeros. At the end we select from the output of RS decoder only **K'** original data bytes. Then these bytes are converted to stream of bits.

Table 4.4: Mandatory channel coding per modulation

Modulation	Uncoded block size (bytes)	Coded block size (bytes)	Overall coding rate	RS code	CC code rate
BPSK	12	24	1/2	(12,12,0)	1/2
QPSK	24	48	1/2	(32,24,4)	2/3
QPSK	36	48	3/4	(40,36,2)	5/6
16-QAM	48	96	1/2	(64,48,8)	2/3
16-QAM	72	96	3/4	(80,72,4)	5/6
64-QAM	96	144	2/3	(108,96,6)	3/4
64-QAM	108	144	3/4	(120,108,6)	5/6

4.3.8 De-randomizer

The stream of bits coming from RS decoder is forwarded to the de-randomizer. The structure and the operation of the de-randomizer is the same of randomizer. That means, that derandomizer is implemented by the PRBS generator, that was explained in randomizer

Encryption

Chapter 5

5.1 Introduction

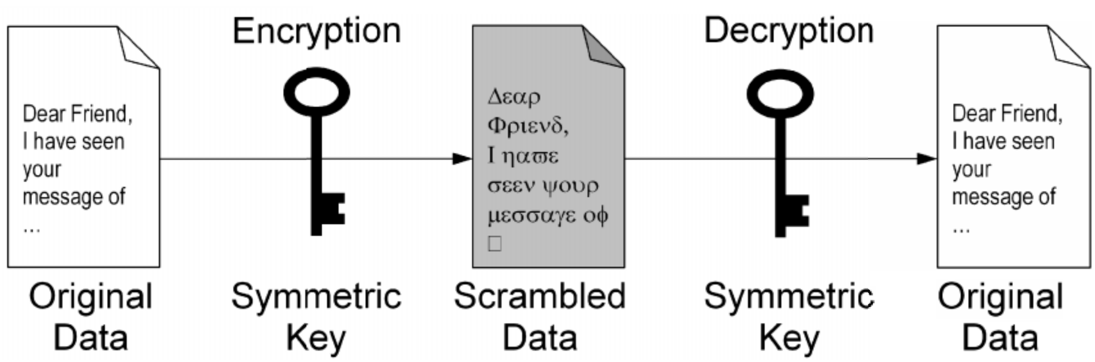


Fig.5.1: Data Encryption Standard (DES)

Security is a broad and complex subject, and this section provides only a brief introduction to it.

We cover the basic security issues, introduce some terminology, and provide a brief overview of some of the security mechanisms, using examples that are relevant to broadband wireless services, especially WiMAX.

The following basic requirements:

- ***Privacy:*** Provide protection from eavesdropping as the user data traverses the network from source to destination.
- ***Data integrity:*** Ensure that user data and control/management messages are protected from being tampered with while in transit.

- ***Authentication:*** Have a mechanism to ensure that a given user/device is the one it claims to be. Conversely, the user/device should also be able to verify the authenticity of the network that it is connecting to. Together, the two are referred to as mutual authentication.

- ***Authorization:*** Have a mechanism in place to verify that a given user is authorized to receive a particular service.

- ***Access control:*** Ensure that only authorized users are allowed to get access to the offered services.

5.2 Attacks, Services, and Mechanisms

There are three aspects considered for information security:

a- Security attack: Any action that compromises the security of information owned by an organization.

b- Security mechanism: A mechanism that is designed to detect, prevent, or recover from a security attack.

c- Security service: A service that enhances the security of the data processing systems and the information transfers of an organization. The service counters the security attacks and makes use of one or more security mechanisms to provide the service.

5.2.1 Security Attacks

The types of attacks on the security of computer systems or communication networks are best characterized by viewing the function of the computer system as providing information or intercepting the flow of information from a source to the destination. There are four general categories of attack:

- ***Interruption:*** An asset of the system is destroyed or becomes unavailable. This is an attack on availability. Examples include destruction of a piece of hardware, such as a hard disk, or cutting of a communication line

- ***Interception:*** An unauthorized party gains access to an asset. This is an attack on confidentiality. The unauthorized party could be a person, a program, or a computer.

- ***Modification:*** An unauthorized party not only gains access to but tampers with an asset. This is an attack on integrity. Examples include changing values in a data file, altering a program so that it performs differently, and modifying the content of messages being transmitted in a network.

- ***Fabrication:*** An unauthorized party inserts false object into the system. This is an attack on authenticity. Examples include the insertion of spurious massages in a network or the addition of records to a file. A useful categorisation of these attacks in terms of passive attacks (wiretapping) which threatens secrecy, and active attacks (wiretapping) which threatens authenticity.

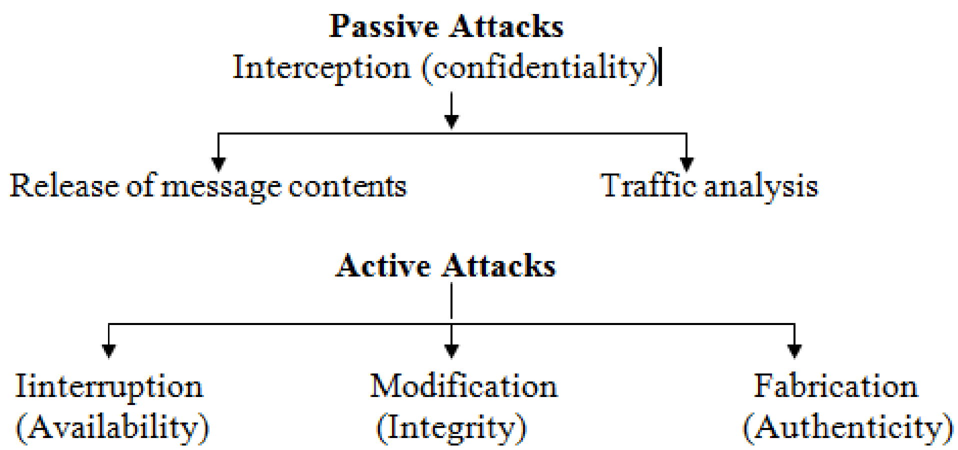


Fig.5.2: Active and Passive Attacks

5.2.1.1 Passive Attacks

Passive attacks are in the nature of eavesdropping on, or monitoring of, transmissions. The goal of the opponent is to obtain information that is being transmitted. Two types of attacks are involved here:

- ***Release of message contents:*** it is easily understood. A telephone conversation, an electronic mail message, a transferred file may contain

sensitive or confidential information. We would like to prevent the opponent from learning the contents of these transmissions.

- ***Traffic analysis*:** it is subtler. Suppose that we had a way of masking the contents of messages or other information traffics so that opponent, even if they captured the message, could not extract the information from the message.

5.2.1.2 Active Attacks

Active attacks (tampering), which threatens authenticity, refers to deliberate modifications made to the message stream. These modifications can be introduced for the purpose of making arbitrary changes to message content or for replacing data in messages with replays of data from earlier messages; also it can be for the purpose of injecting false messages or deleting messages. Active attacks can be divided into four categories:

- ***Masquerade:*** takes place when one entity pretends to be a different entity. For example, authentication sequences can be captured and replayed after a valid authentication sequence has taken place.
- ***Replay:*** involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect.
- ***Modification:*** of messages means that some portion of a legitimate message is altered or those messages are delayed or reordered, to produce an unauthorized effect.
- ***Denial of service***: means preventing or inhibiting the normal use or management of communications facilities. This attack may have specific target; for example, an entity may suppress all messages directed to a particular destination.

5.2.2 Security Services

- ***Confidentiality:*** is the protection of the transmitted data from passive attacks. Several levels of protection can be identified. The broadest service protects all user data transmitted between two users over a period of time. The other aspect of confidentiality is the protection of traffic flow from analysis. This requires that an attacker cannot be able to observe the source

and the destination, frequency, length, or other characteristics of the traffic on the communication facility.

- ***Authentication:*** The authentication service is concerned with assuring that a communication is authentic. Also the service must assure that the connection is not interfered with, in such a way that a third party can masquerade as one of two legitimate parties for the purposes of unauthorized transmission or reception.

- ***Integrity:*** A connection-oriented integrity service assures that messages are received as sent with no duplication, insertion, modification, or replays. Thus, the connection-oriented integrity service addresses both message stream modification and denial of service.

- ***Access Control:*** In network security, access control is the ability to limit and control the access to the host systems and applications via communication links. To achieve this control, each entity trying to gain access must first be identified, or authenticated, so that access rights can be tailored to the individual.

- ***No repudiation:*** It prevents either sender or receiver from denying a transmitted message. Thus, when message is sent, the receiver can prove that the alleged sender in fact sent the message. Similarly, when a message is received, the sender can prove that the alleged receiver in fact received the message.

5.2.3 Mechanisms

Mechanisms which support key establishment and the maintenance of ongoing keying relationships between parties, including replacing older keys with new keys as necessary.

Key establishment can be broadly subdivided into key agreement and key transport. Many and various protocols have been proposed to provide key

establishment. Simple architectures based on symmetric key and public-key cryptography along with the concept of certification will be addressed.

The key management problem is a crucial issue. There are a number of ways to handle this problem. Two simplistic methods are discussed; one based on symmetric-key and the other on public-key techniques.

5.3 DES Algorithm

The DES block cipher algorithm was developed by researchers at IBM and was fine-tuned by government agencies, the National Security Agency (NSA) and the National Institute of Standards and Technology (NIST). The American National Standards Institute (ANSI) adopted DES as the federal standard for encryption of commercial and sensitive data. This is defined in Federal Information Processing Standards (FIPS 46, 1977) published by NIST[1], [2].

5.3.1 DES Structure

The DES algorithm has a regular structure that lends itself to pipelining and simple data manipulations to permit fast operations. DES is a symmetric encryption algorithm where the same key is used for both encryption and decryption. DES takes a 64-bit key and a 64-bit block of data as inputs, and outputs 64-bits of encrypted data. The actual key is only 56-bits and the remaining bits, i.e., the least significant bit (LSB) in every byte can be used as parity.

The DES algorithm had two major weaknesses:

- ***Key size:*** 56 bits may have not provided adequate security.
- ***S-boxes:*** The S-boxes may have hidden trapdoors.

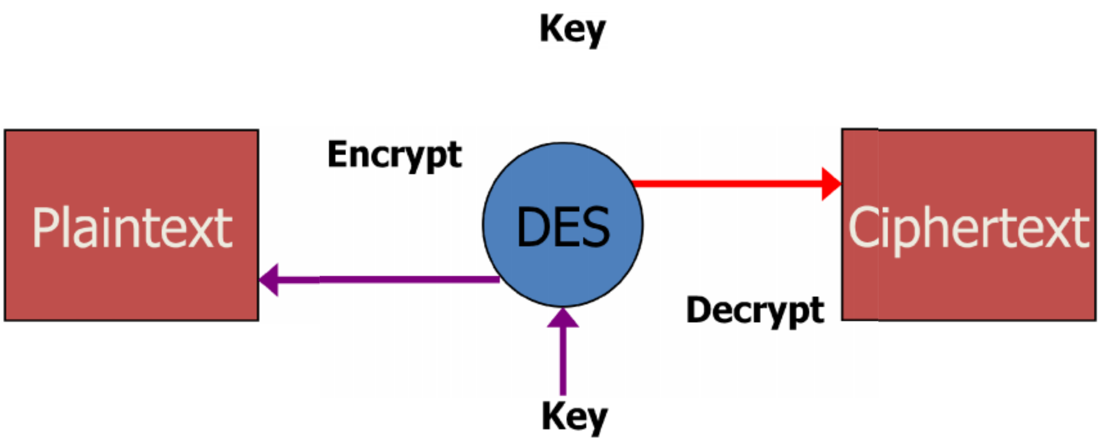


Fig.5.3: Symmetric system

5.3.2 DES Encryption

As shown in Figure 4.3, the DES algorithm begins with an initial permutation (IP), encrypts in sixteen "rounds", followed by the inverse of the initial permutation (IP–1). In each round, the right-side 32 bits of the block are transformed with the function labeled "f" and the key, then XOR with the left-side 32 bits.

Let the 64 bits of the input block to an iteration consist of a 32-bit block L, followed by a 32-bit block R. Using this notation, the input block is then LR. Let K be a block of 48 bits chosen from the 64-bit key. Then, the output L'R' of iteration with input LR is defined by:

The key for each round is a subset of the original 64-bit key with bits permuted. At each iteration, a different block K of key bits is chosen from the 64-bit key designated by KEY. Let KS be a function which takes an integer n in the range from 1 to 16 and a 64-bit block KEY as input.

This yields 48-bit block output Kn which is a permuted selection of bits from KEY; with K_n determined by the bits in 48 distinct bit positions of KEY.

KS is called the key schedule, because the block K used in the nth iteration of equation 1 is the block K_n determined by equation 2. For the nth iteration, left and

right blocks are defined by: where n is in the range of 1 to 16. The pre-output block is R16 L16**.**

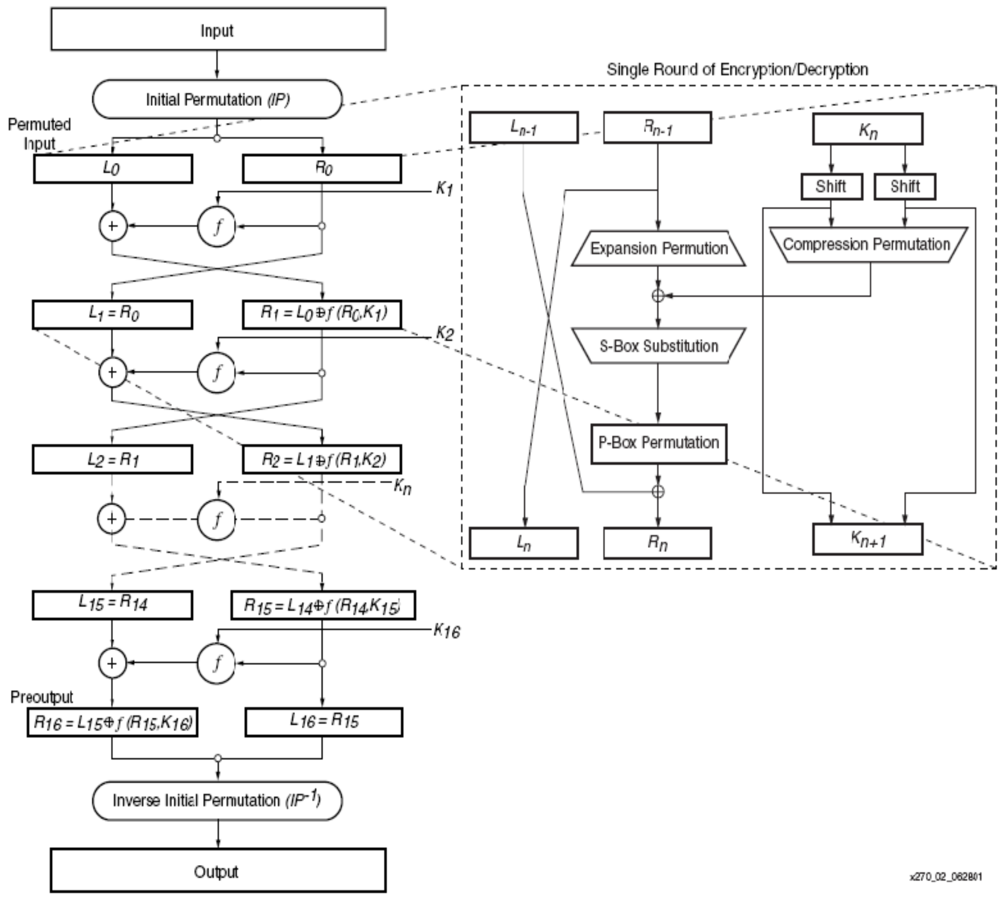


Fig.5.4: *DES encryption*

Initial permutation IP:

Table 4.1: *Initial Permutation*

58	50	42	34	26	18	10	2	60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6	64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1	59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5	63	55	47	39	31	23	15	7

The "f" function expands the right side (Rn) to 48 bits, XOR's those bits with the key, and divides the resulting 48 bits into eight 6-bit fields. Those fields are used as addresses into eight 64-word by 4-bit memories, called S-boxes. The eight 4-bit S-box outputs are re-assembled into the 32-bit word and the bits permuted (P) and XOR with the left side (Ln) of the block. This is illustrated in Figure 4.5.

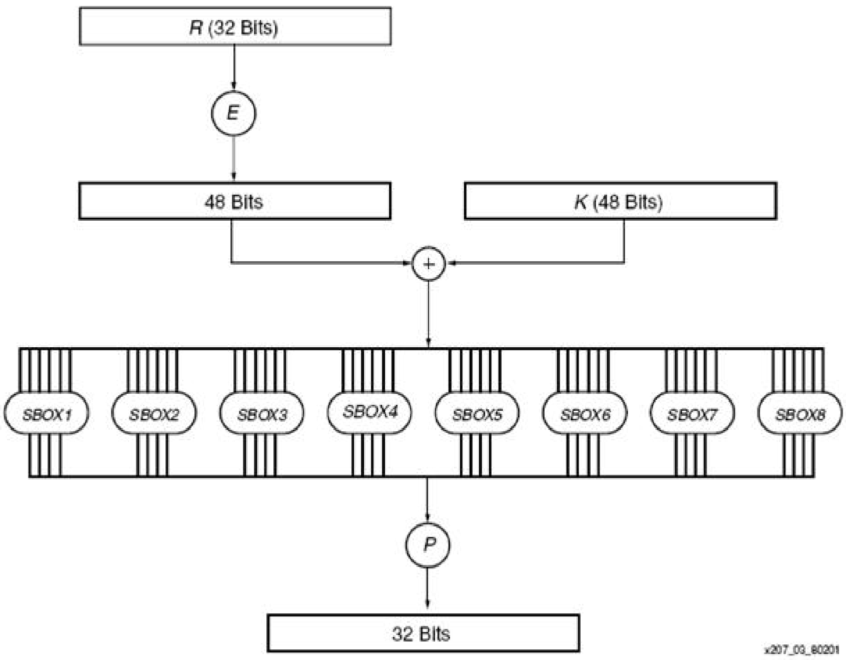


Fig.5.5: *Cipher function*

Inverse of the initial permutation (IP–1):

Table 5.2: *Inverse Initial Permutation*

40	8	48	16	56	24	64	32	39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30	37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28	35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26	33	1	41	9	49	17	57	25

5.3.3 Sub-Key Generation

The Key calculation is shown in Figure 5.5. The input KEY goes through the initial key permutation choice, PC–1. In Figure 2.5, C0 represents 32 MSB bits and D0 represents 32 LSB **bits of PC–1.**

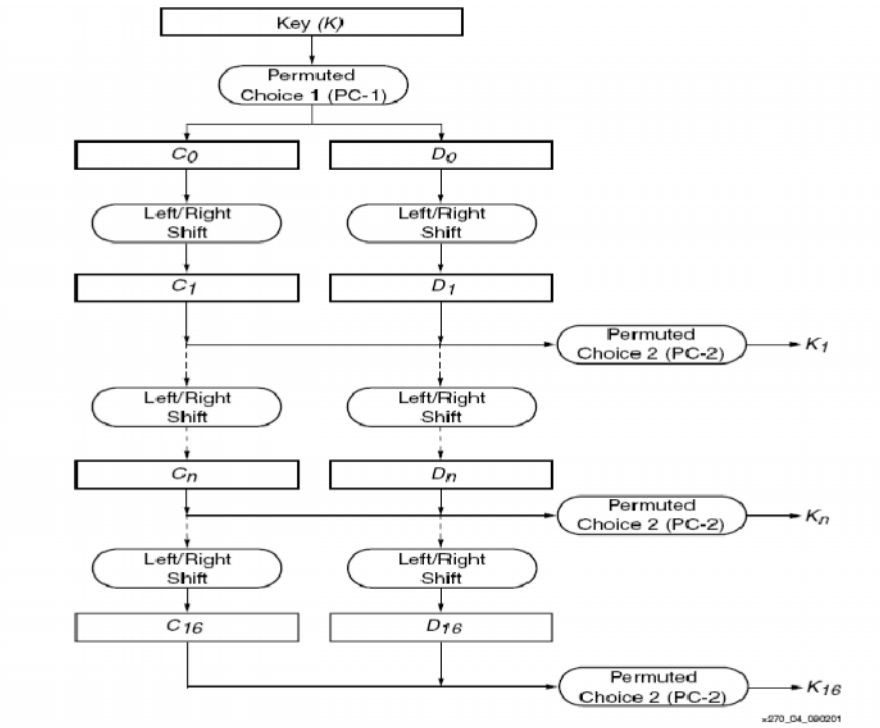


Fig.5.6: Key Function

5.3.4. DES Decryption

The decryption operation is the same as encryption, but the sub keys Kn are presented in the opposite order. In hardware, this amounts to changing the direction of shift and the shift amounts in sub-key generation. The permutation IP–1 applied to the pre-output block is the inverse of the initial permutation IP applied to the input. Further, from equation 1 it follows that:

Consequently, to decrypt the message it is only necessary to apply the very same algorithm to an encrypted message block. At each iteration of the computation the same block of key bits K is used during decryption as was used during the encryption of the block. Using the notation of the previous section.

Now R16L16 is the permuted input block for the decryption calculation and L0R0 is the pre output block. That is, for the decryption calculation with R16L16 as the permuted input, K16 is used in the first iteration, K15 in the second, and so on, with K1 used in the 16th iteration.

In summary, the DES algorithm consists of 16 identical encryption rounds. Each round contains a significant amount of bit movement, which is simple wire in a hardware implementation, 80 2-bit XORs, and eight lookups in 64-word by 4-bit S-boxes. Each round uses a subset of the key bits with a particular permutation. The permutation depends on the round and on whether the operation is to encrypt or decrypt. This primarily involves wiring, table lookups, and bitwise operations. FPGAs are best suited for such operations and form an ideal platform for DES implementation.

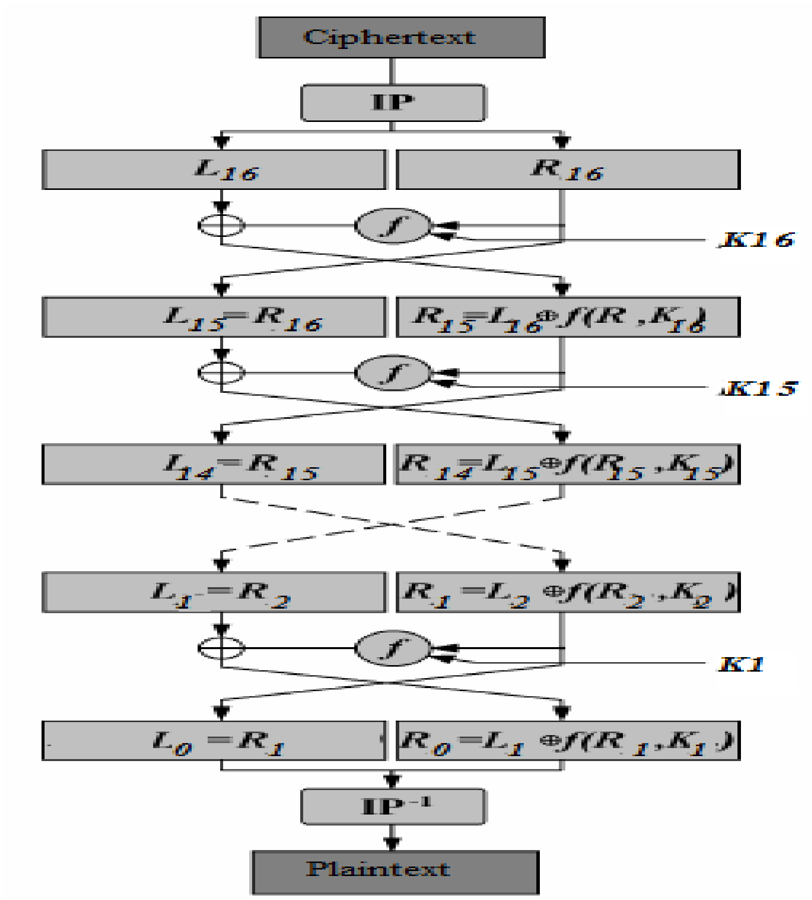


Fig.5.7: DES Decryption

Implementation of PHY WiMAX by VHDL

Chapter 6

6.1 FPGA Overview

6.1.1 General Description

There are two basic types of FPGAs:

• SRAM-based reprogrammable and One-Time Programmable (OTP).

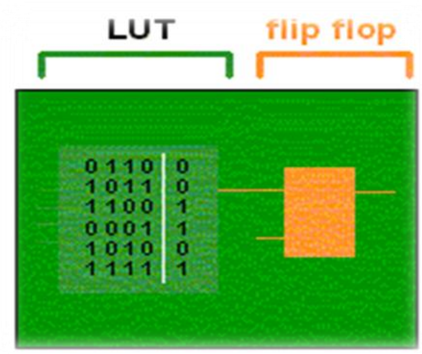


Fig.6.1: SRAM

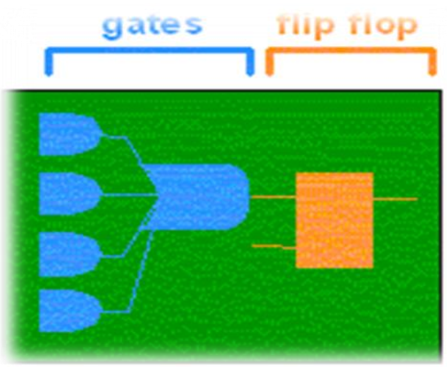


Fig.6.2: OTP

These two types of FPGAs differ in the implementation of the logic cell and the mechanism used to make connections in the device.

The dominant type of FPGA is SRAM-based and can be reprogrammed as often as you choose. In fact, an SRAM FPGA is reprogrammed every time it's powered up, because the FPGA is really a fancy memory chip. That's why you need a serial PROM or system memory with every SRAM FPGA.

- SRAM logic cell, instead of conventional gates, an LUT determines the output based on the values of the inputs. (In the "SRAM logic cell" diagram above, six different combinations of the four inputs determine the values of the output.) SRAM bits are also used to make connections.

- OTP FPGAs use anti-fuses (contrary to fuses, connections are made, not “blown,” during programming) to make permanent connections in the chip.

Thus, OTP FPGAs do not require SPROM or other means to download the program to the FPGA.

6.1.2 Development Board Hardware I/O Features

Each of the FPGA boards has a slightly different feature set of logic, I/O interfaces, memory and other assorted hardware. As long as the FPGA board has enough logic and it has the required I/O features, a project can be implemented on any of the boards.

FPGAs are available in a wide range of sizes with different feature sets. In general, FPGAs with more logic, more I/O pins, higher speed, or more memory are more expensive. When designing new products, choosing the FPGA with the proper feature set at the lowest cost is an important design consideration.

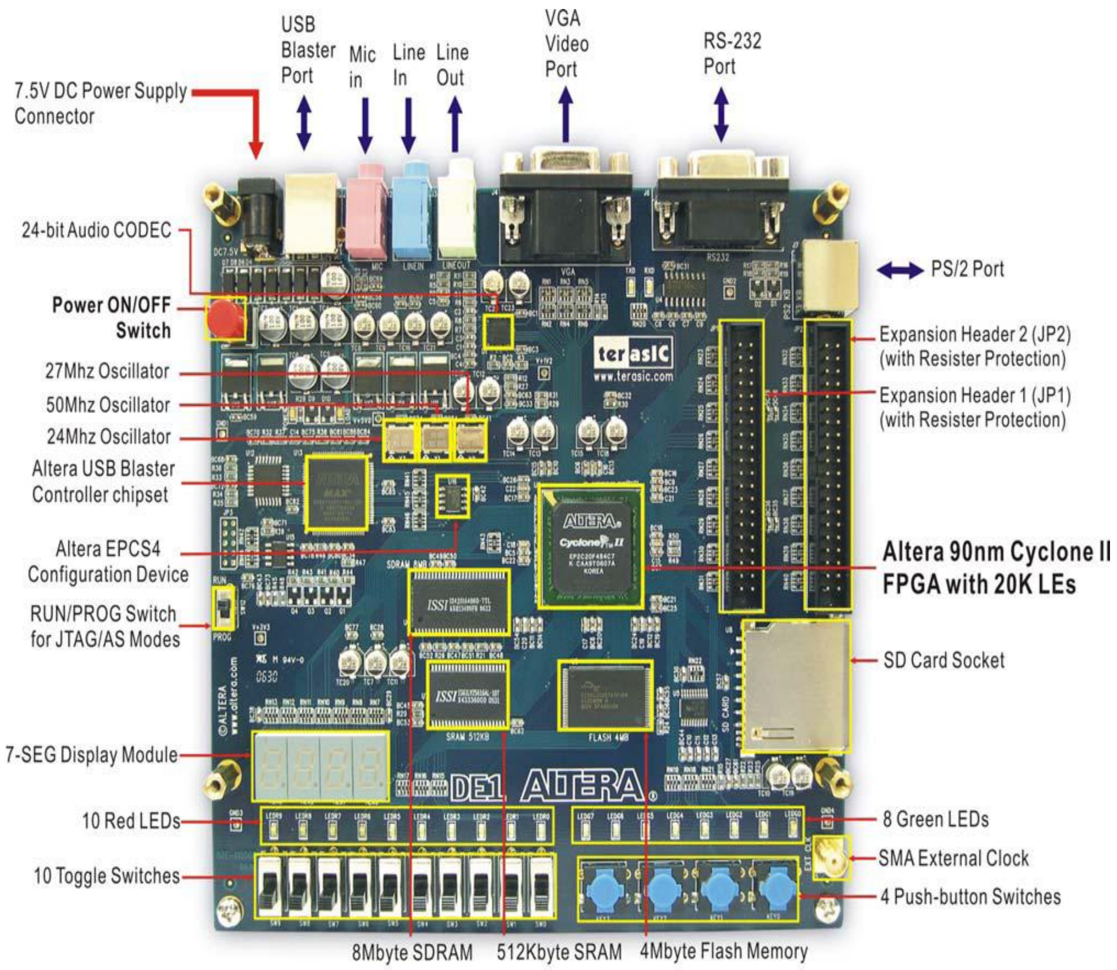
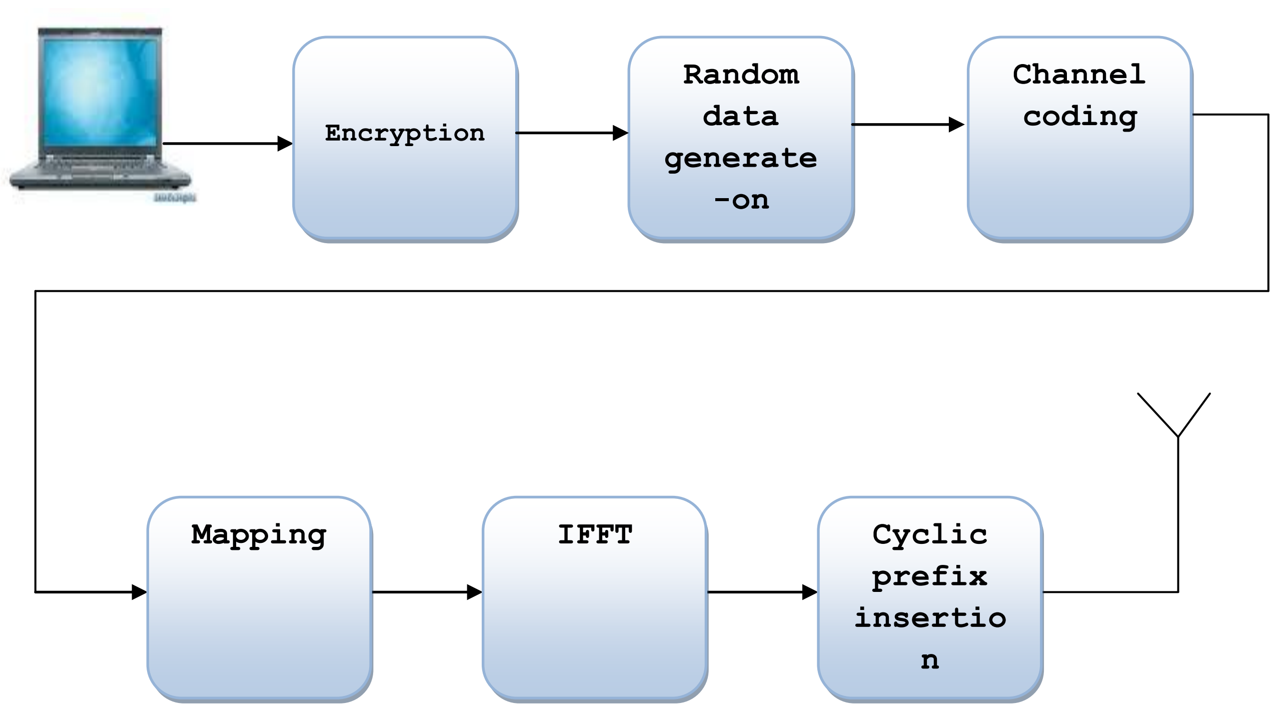


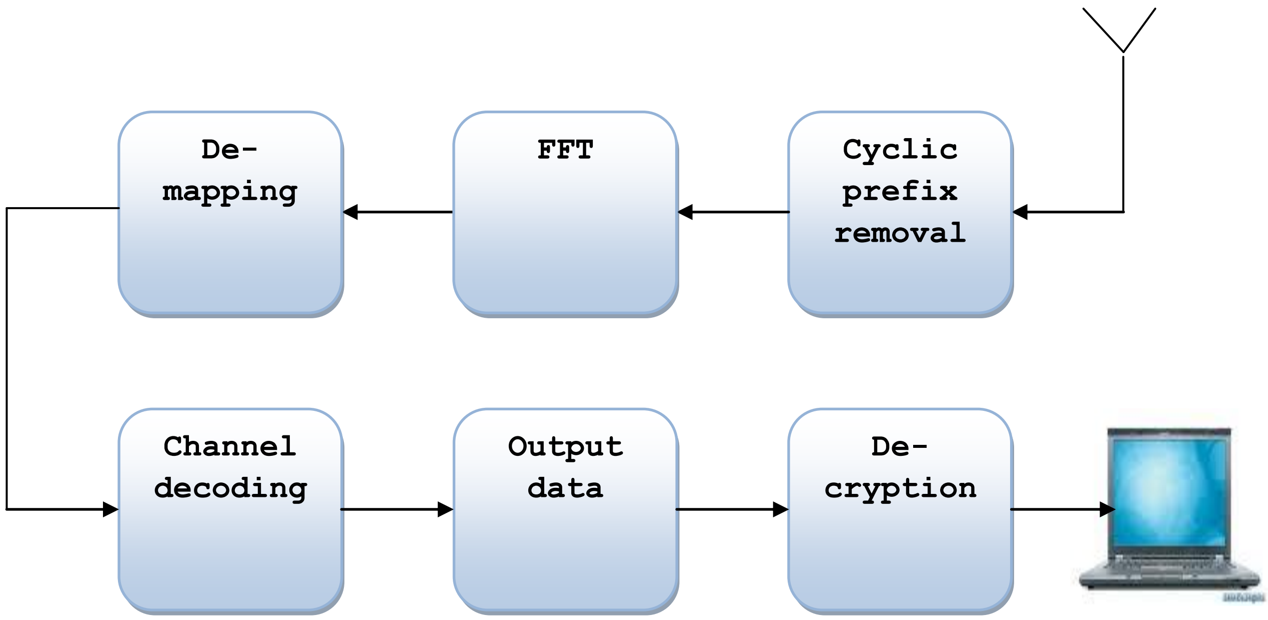
Fig.6.3: *FPGA KIT I/O features*

6.2 Software WiMAX PHY

Transmitter:

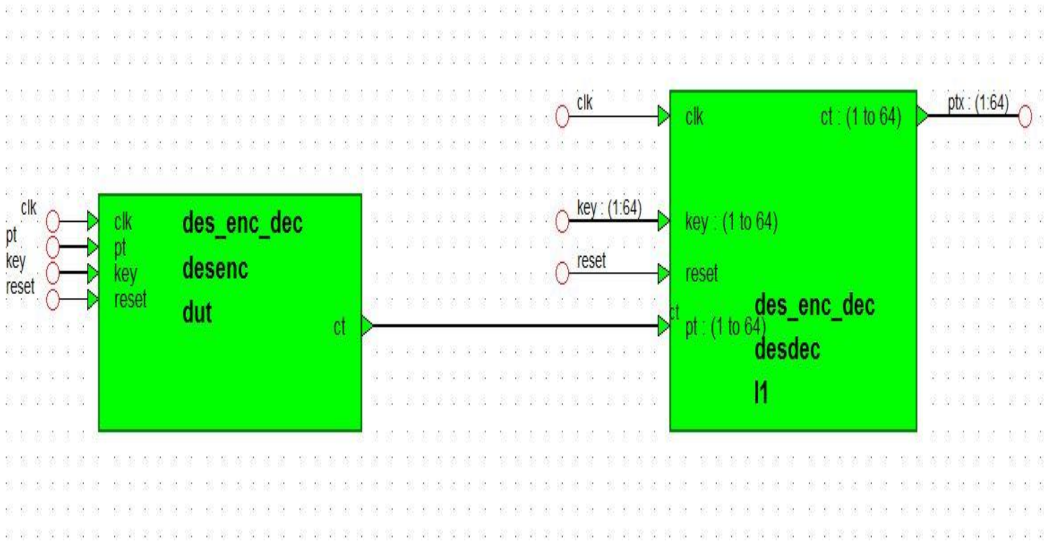


Receiver:



6.2.1 Encryption & Decryption

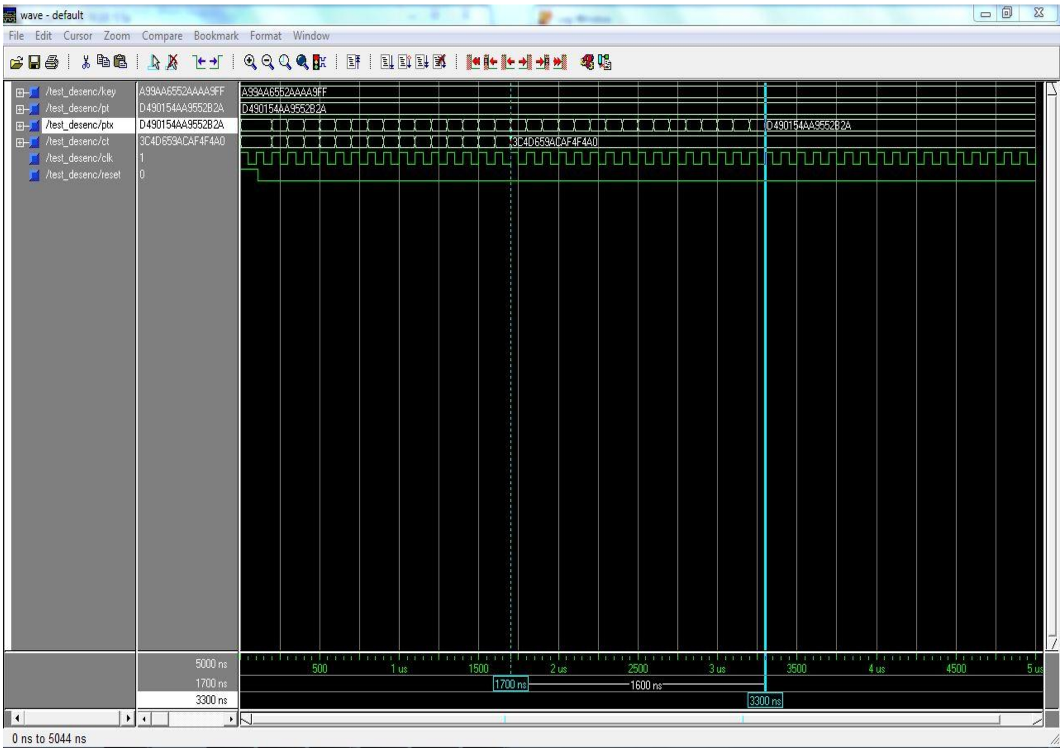
VHDL Block Diagram:



INPUT: pt, key, (64 bit) ; clk, reset(1 bit) .

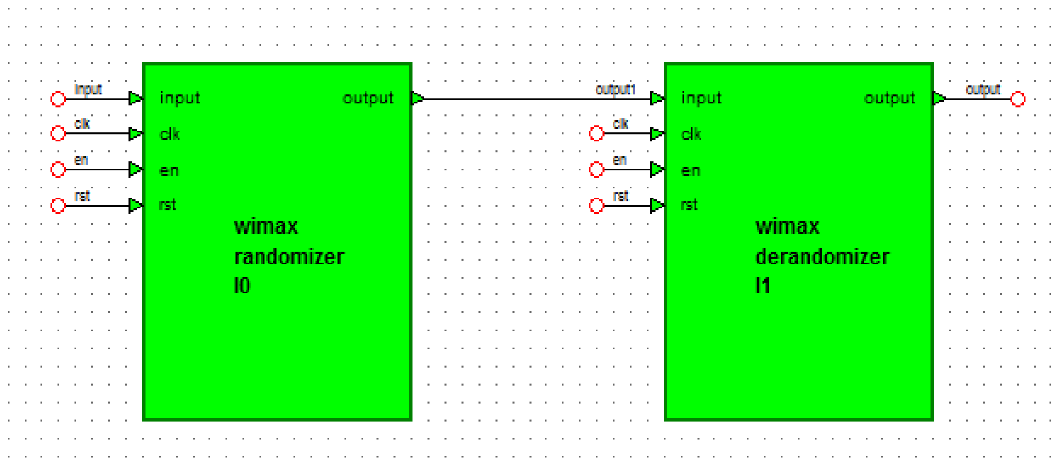
OUTPUT: ptx (64 bit).

Simulations:



6.2.2 Randomizer & Derandomizer

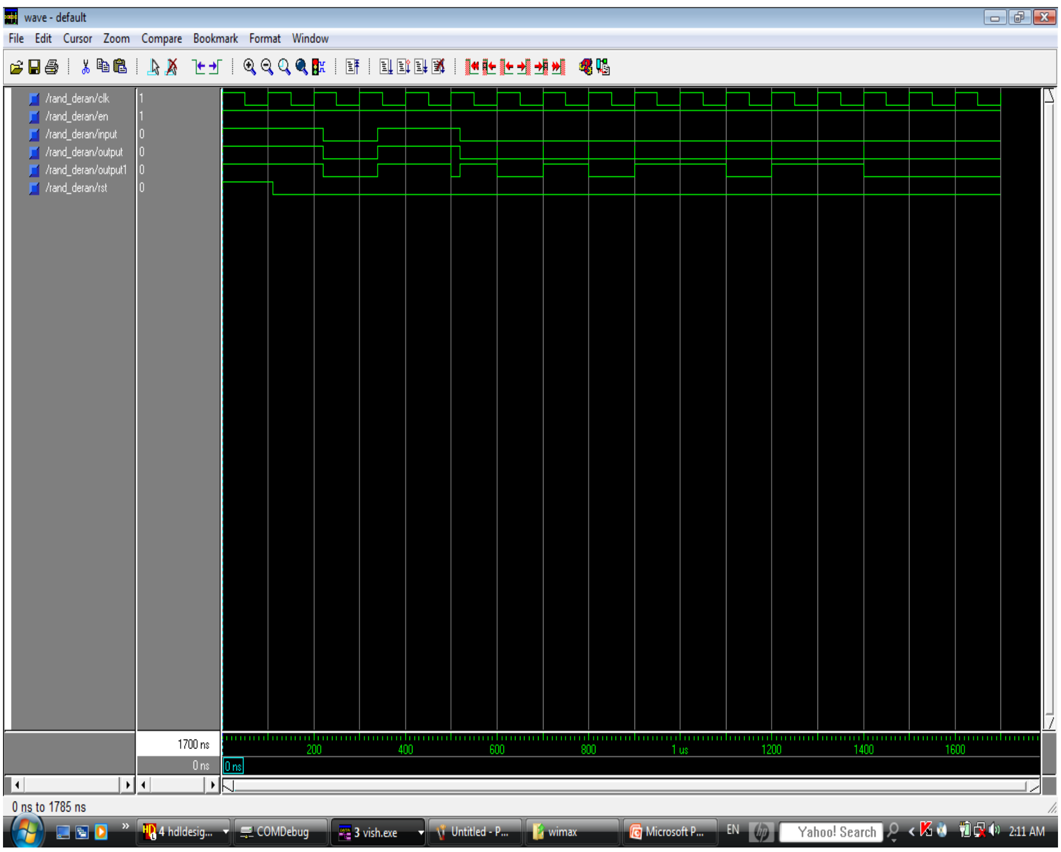
VHDL Block Diagram:



INPUT: input, clk, en, rst (1 bit).

OUTPUT: output (1 bit).

Simulations:



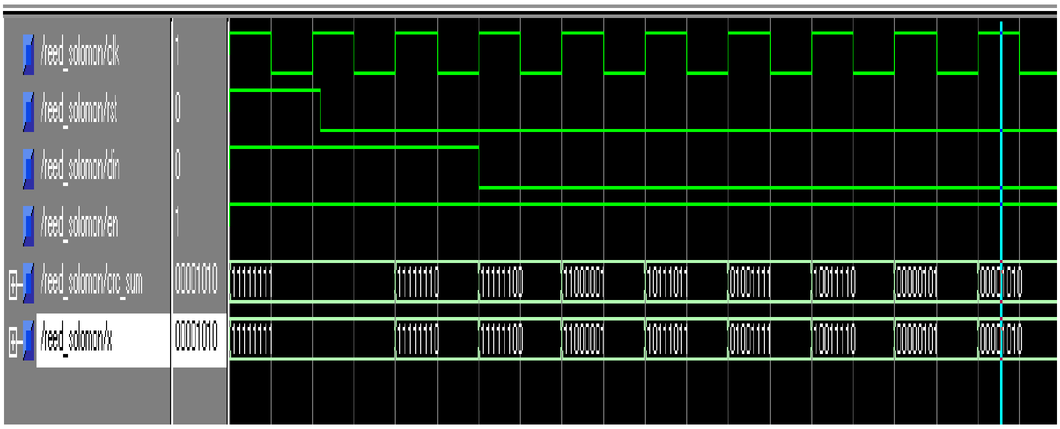
5.2.3 Reed Solomon

VHDL Block Diagram:

INPUT: x (8 bit).

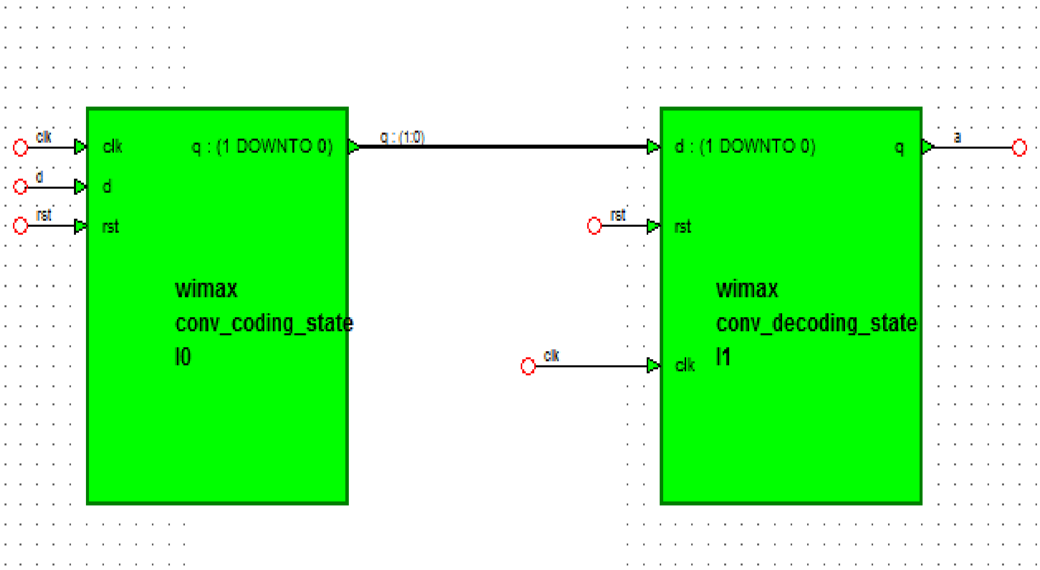
OUTPUT: y (14 bit).

Simulations:



6.2.4 Convolution Coding and Decoding

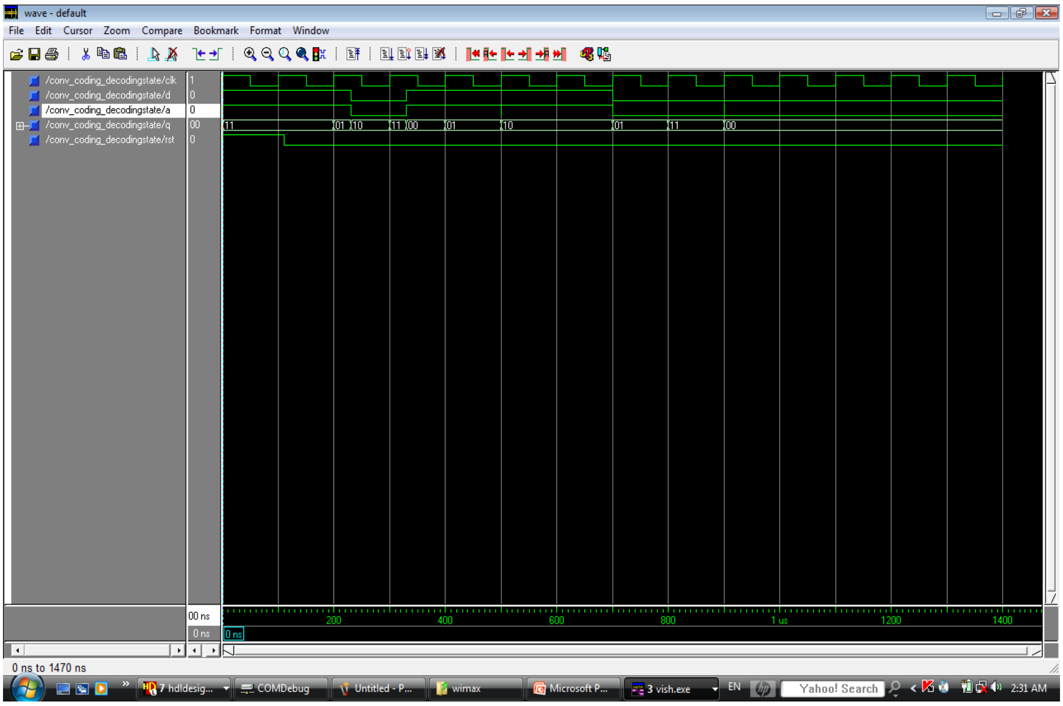
VHDL Block Diagram:



INPUT: clk, d, rst (1 bit).

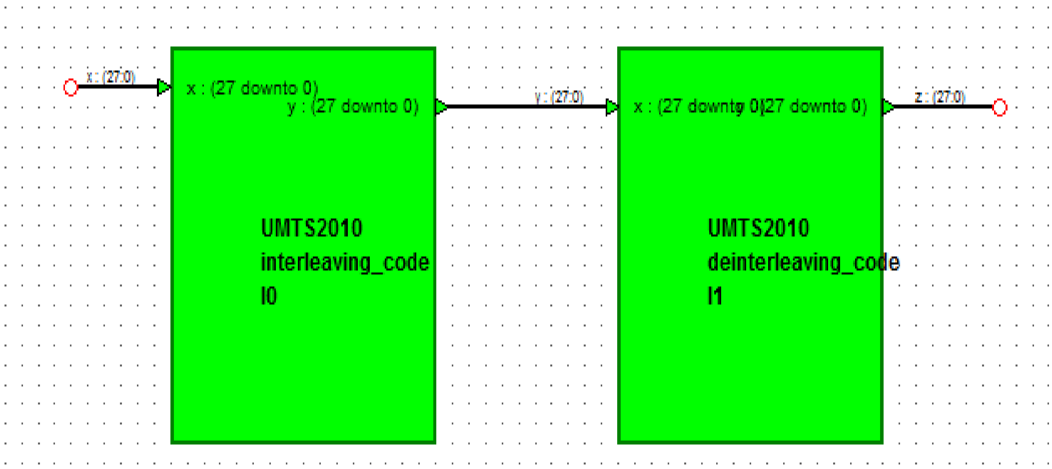
OUTPUT: a (1 bit).

Simulations:



6.2.5 Interleaving & De-interleaving

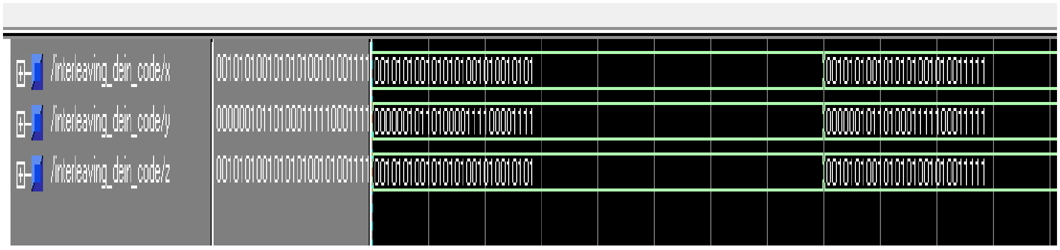
VHDL Block Diagram:



INPUT: x (28 bit).

OUTPUT: z (28 bit).

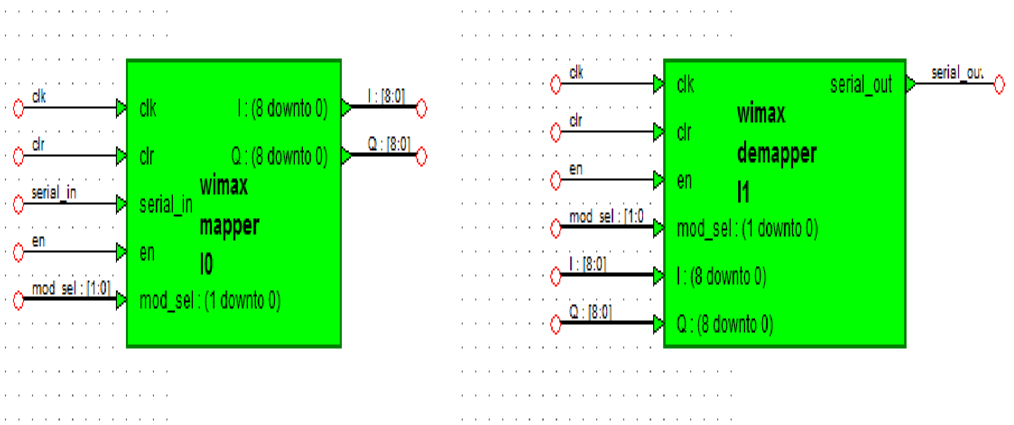
Simulations:



6.2.6 Mapping

VHDL Block Diagram:

WiMAX mapper:



INPUT: clk, dr, serial_in, en (1 bit) ; mod_sel (2 bit) .

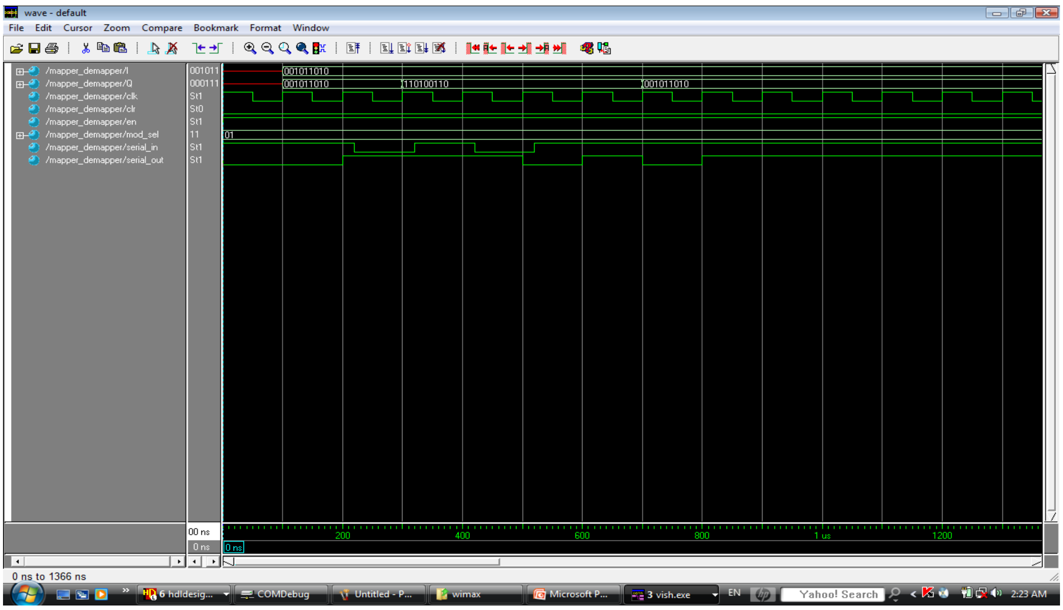
OUTPUT: I, Q (9 bit).

WiMAX demapper:

INPUT: clk, dr, en (1 bit) ; mod_sel (2 bit) ; I, Q (9 bit).

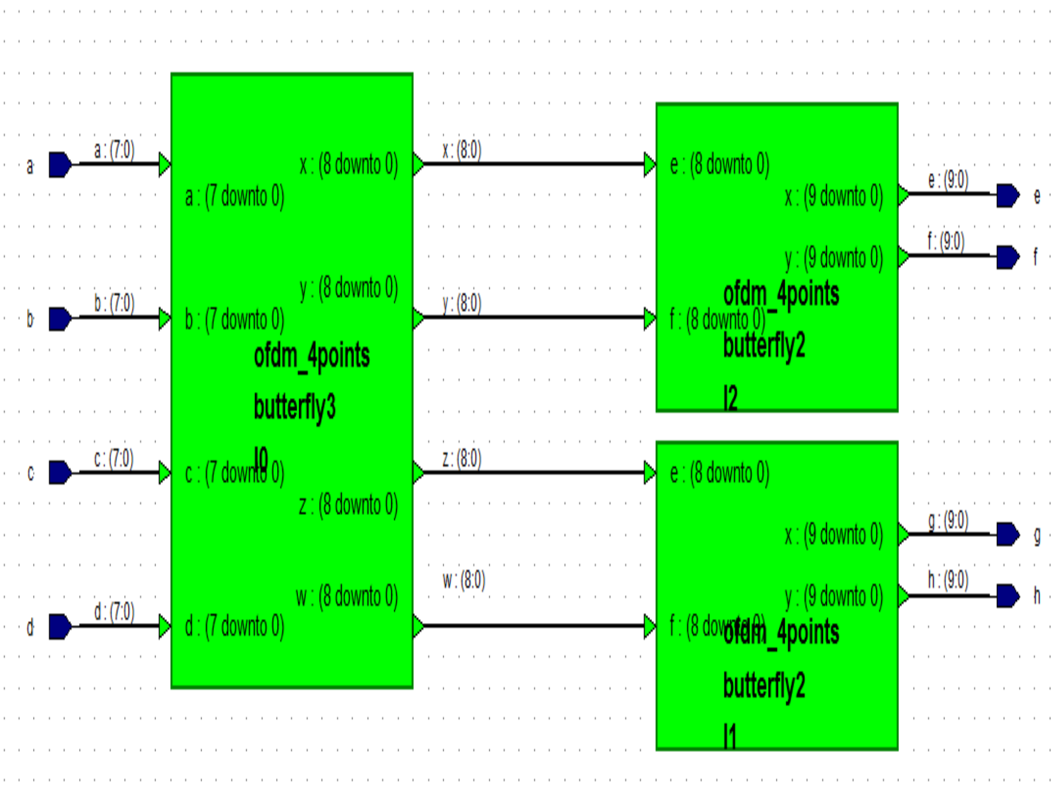
OUTPUT: serial_out (1 bit).

Simulations:



6.2.7 IFFT & FFT

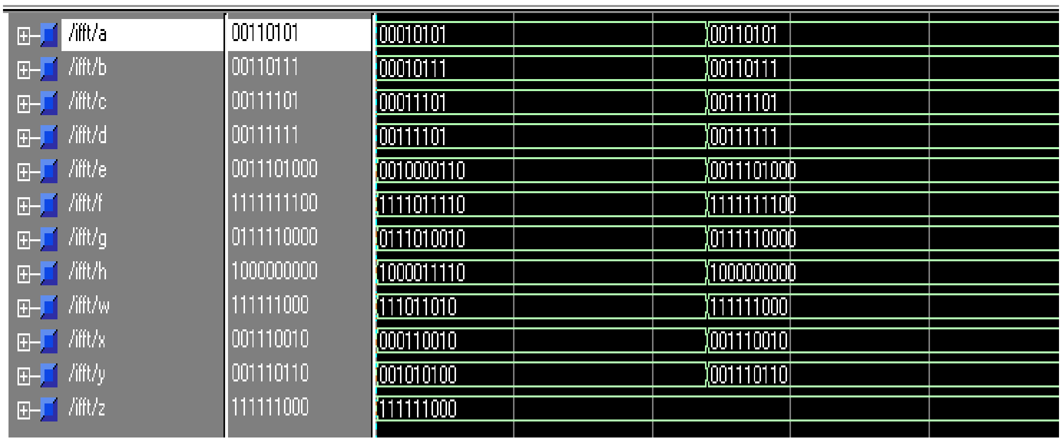
VHDL Block Diagram: (VHDL IFFT)



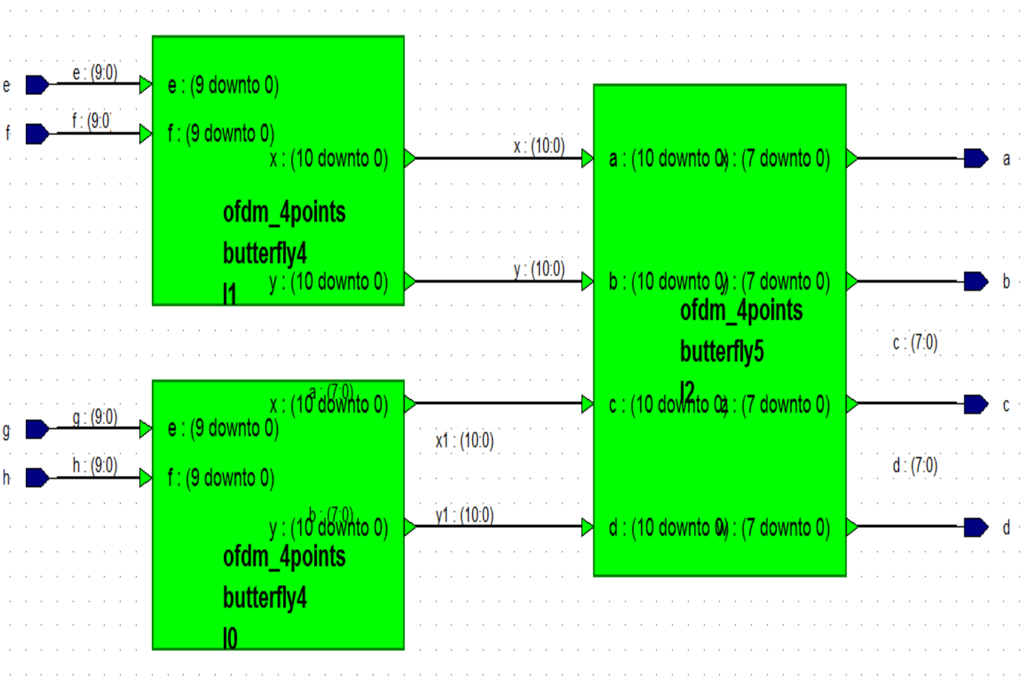
INPUT: a, b, c, d (8 bit).

OUTPUT: e, f, g, h(10 bit).

Simulations: (Simulation IFFT)



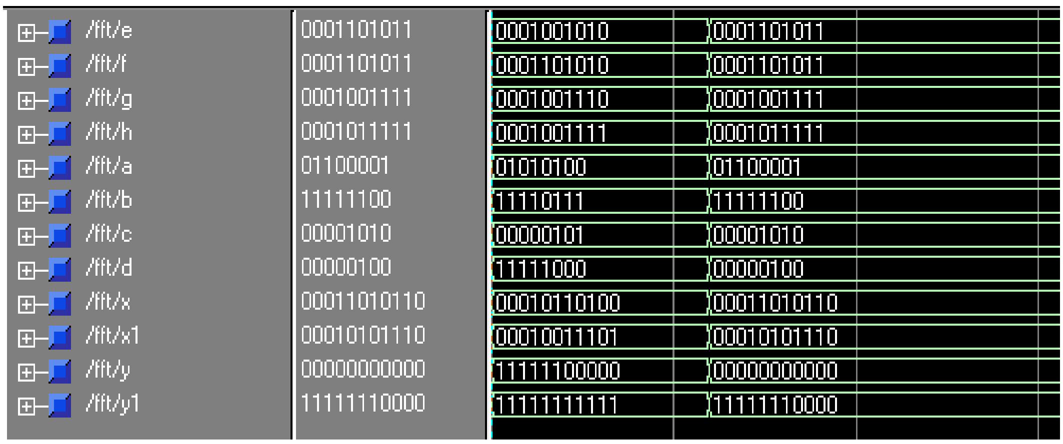
VHDL Block Diagram: (VHDL FFT)



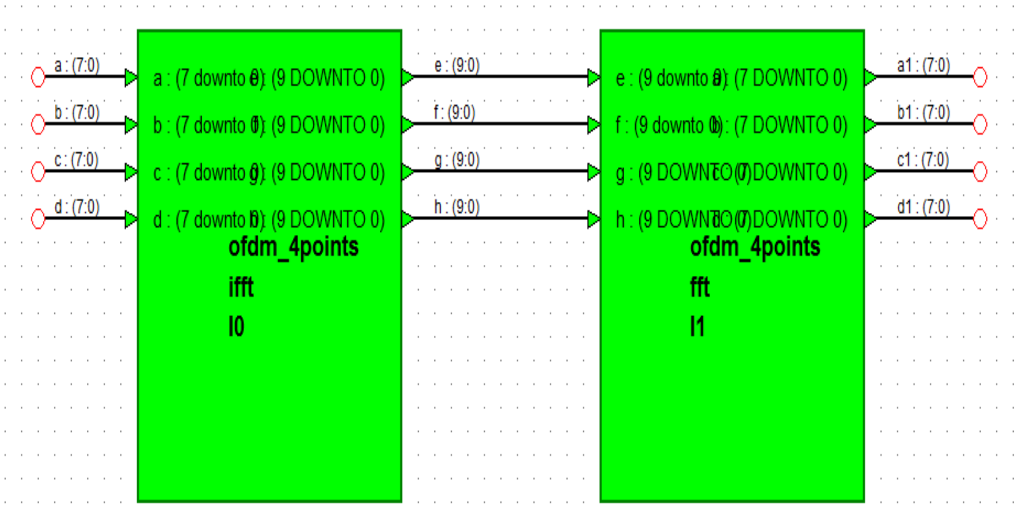
INPUT: e, f, g, h (10 bit).

OUTPUT: a, b, c, d (8 bit).

Simulations: (Simulation FFT)



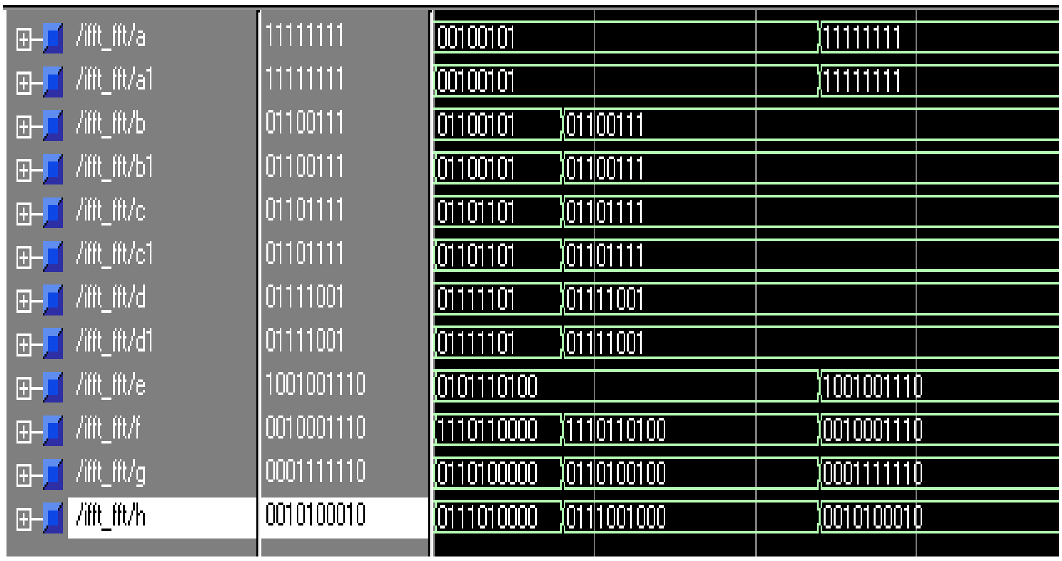
VHDL Block Diagram: (VHDL IFFT,FFT)



INPUT: a, b, c, d (8 bit).

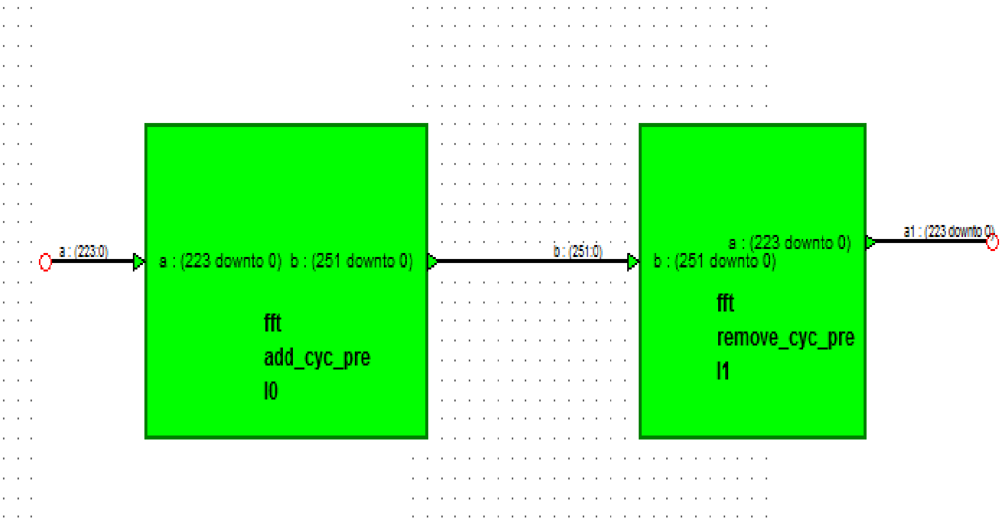
OUTPUT: a1, b1, c1, d1 (8 bit).

Simulations: (Simulation IFFT,FFT)



6.2.8 Cyclic Prefix

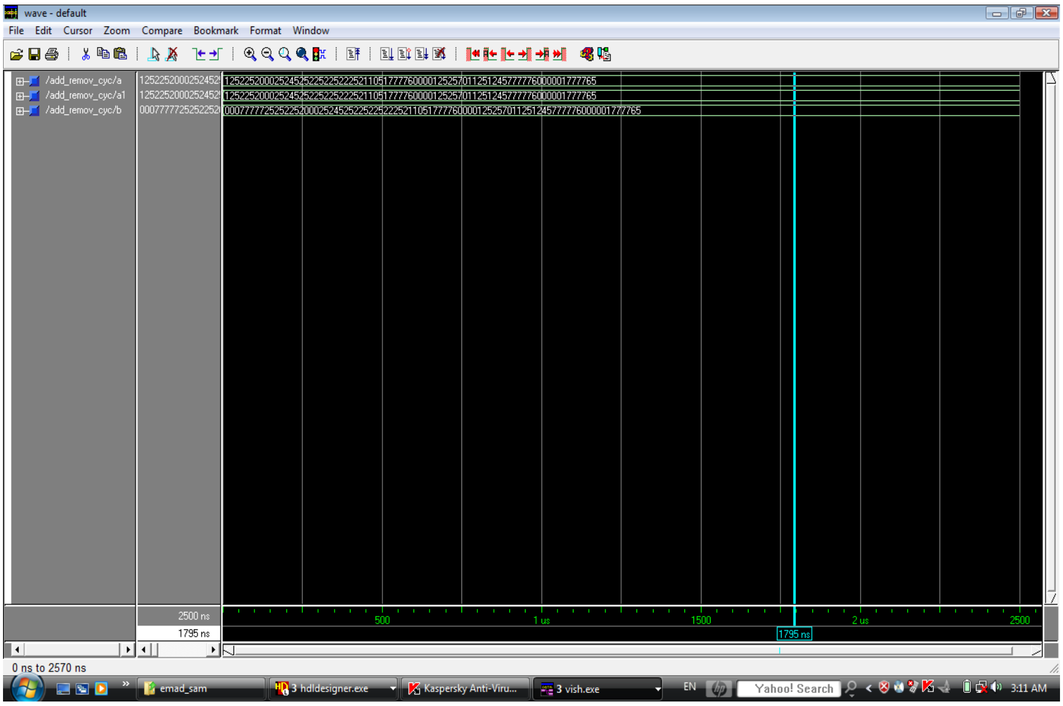
VHDL Block Diagram:



INPUT: a (224 bit).

OUTPUT: a1 (224 bit).

Simulations:



Conclusions and suggestions of future work

Chapter 7

7.1 Introductions

In this project we studies the "mobile WiMAX" that is based on IEEE 802.16e-2005 and "Fixed WiMAX" that based on IEEE 802.16d-2004 and target mobile and nomadic subscribers in wireless metropolitan area network (WMAN) and studied the PHY WiMAX and implementation PHY WiMAX by VHDL.

7.2 Conclusions

In this project we studied the PHY WiMAX and implementation PHY WiMAX. The following blocks were discussed and convert to VHDL codes:

- Encryption & De-encryption.
- Randomizer & De-randomizer.
- Read Solomon encoding an & Read Solomon decoding
- Convolution encoding & Convolution decoding.
- Interleaving & De-interleaving.
- Mapping & De-mapping.
- IFFT & FFT.
- Cyclic prefix insertion & Cyclic prefix removal.

We conclusions that:

- The function of each block.
- The benefits of each block.
- The reach of PHY WiMAX system and how can work by VHDL.
- Implementation the security in system and reach to cipher plain.

In this project work, the mandatory of WiMAX transceiver is described and implemented based on the IEEE 802.16 OFDM PHY layer standard. VHDL Is used to do so. The goal was to calculate the performance of PHY layer. The model can support all types of modulation with different code rates. In this model, we have assumed that the receiver and the transmitter are completely synchronized. This project work can be extended by using the optional block turbo coding (BTC) in order to improve the performance of FEC.

7.3 Suggestions for future work

7.3.1 WiMAX future

IEEE 802.16d (fixed WiMAX) and IEEE 802.16e(mobile WiMAX) available in USA, UK, Spain, France, Germany, South Korea and many countries. But the expectable to implement in the next years is IEEE 802.16m which will achieve the IMT-Advanced 2000.

7.3.1.1 IMT-2000 & IMT-Advanced

IMT-Advanced, also known as "systems beyond IMT-2000" is expected to offer constant higher data rates with high mobility to assure likely growing need for mobile WiMAX services that goes beyond what IMT-2000 can afford to provide. IMT- Advanced is awaiting technology that will require 3 to 5 years in the future with target maximum data rates, for research and examination, of up to 100 Mbits/sec in high mobility applications and up to 1 Gbit/sec in low mobility or nomadic applications. The capacity expected by IMT-Advanced is often referred to as 4G. It is commonly acknowledged that Orthogonal Frequency Division Multiple Access (OFDMA) technology will be integrated in IMT-Advanced in near future to get more the maximum benefits from the WiMAX.

IMT-Advanced is a continuing effort. The full criteria, being extended within ITU-R Working Party 8F, are not expected until 2008. The specification of IMT-Advanced technologies will probably not be completed until at least 2010. In preparation for IMT-Advanced, the IEEE 802.16 Working Group has moved to initiate a new project designated as "802.16m" with the intent of developing enhancements to IEEE STD 802.16 to ensure suitability as an IMT-Advanced proposal.

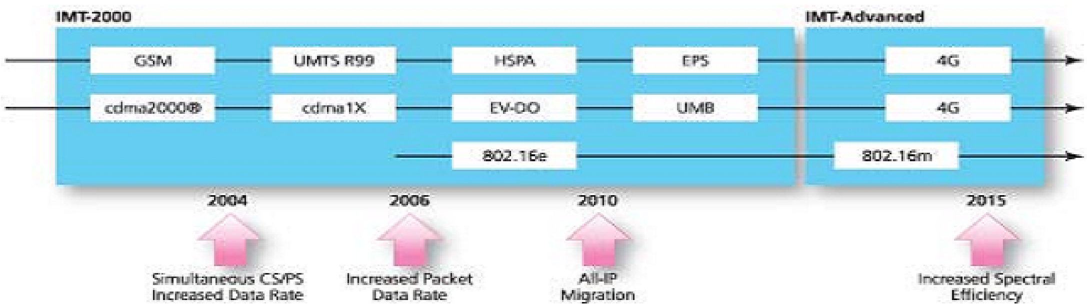


Fig.7.1: *IMT-2000 & IMT-Advanced*

7.3.1.2 IEEE 802.16m goals

- Increase system capacity
- Coverage improvement (at cell edge)
- Reduce MAC overhead
- Mobile client power efficiency
- Enhance mobility
- Improve Quality of Service
- Meet IMT-Advance Standard requirements (not yet defined)
- It will also be 4G compatible with the future wireless networks offering much higher speeds.

7.3.1.3 802.16m specifications.

- Amendment for advanced air interface.
- Looking to the future.
- It is anticipated that it will provide:

1. Data rates of 100 Mbps for mobile applications and 1 Gbps for fixed applications.
2. Cellular, macro and micro cell coverage.
3. 16m and 16e shall be able to operate on the same RF carrier, with the same/different channel bandwidth
4. Operating frequencies: less than 6 GHz
5. Operating bandwidths: 5 to 20 MHz and more.
6. Duplex schemes: TDD and FDD, HFDD
7. Modulation (OFDMA - downlink and uplink), support smart antennas

7.3.1.4 IEEE 802.16m & LTE

LTE stands for long term evolution.

LTE is a set of enhancements to the Universal Mobile Telecommunications System (UMTS) which will be introduced in 3rd Generation Partnership Project (3GPP) Release 8 in March 2009.

Much of 3GPP Release 8 will focus on adopting 4G mobile communications technology.

- Both LTE and IEEE 802.16m are all IP networks based on OFDM technology.
- Both support FDD and TDD.
- Both support higher order MIMO antenna solutions.
- In contrast to the forthcoming first generation LTE
- there have already been two releases of WiMAX profiles:

1. the IEEE 802.16d fixed WiMAX standard released in 2004
2. the IEEE 802.16e mobile WiMAX standard released in 2005

Both of those standards have been implemented and there are compliant networks and devices/ products available.

- As for speeds, LTE will be faster than the current generation of WiMax, but 802.16m that should be ratified in 2009 is fairly similar in speeds.
- New spectrum required for either LTE or WiMAX to support wider channel BW MultiBand/Multi-Mode subscriber devices required in either case for internetwork connectivity and global roaming

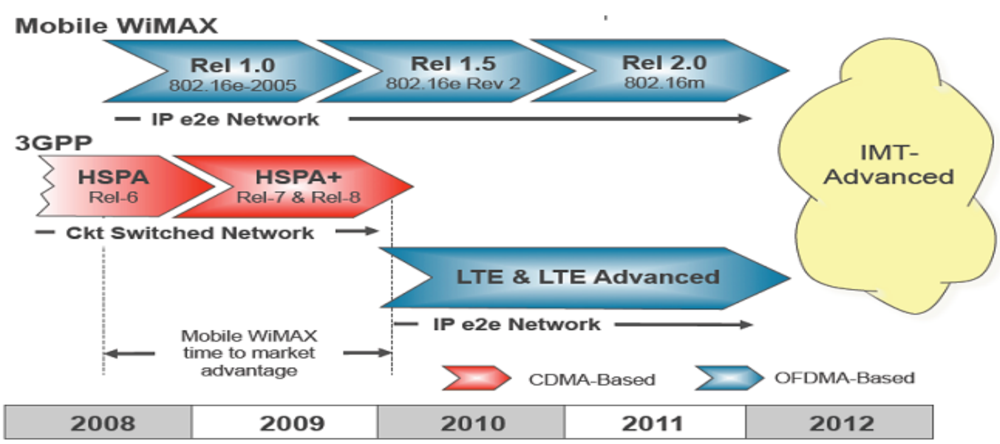


Fig.7.2: 3GPP & Mobile WiMAX Timeline

7.3.2 Mobility management suggestions

Ability to make the user to put the MS in any part and the program can detect the appropriate action and execute it.

7.3.3 Hardware suggestions

- Improving sensitivity of circuit by replacing some components by other has a low tolerance and adding some circuits to decrease noise.
- Design a selectivity system to select a certain band of frequency by adding band pass filter.
- Changing display by LCD to add some features and information.

Appendix

Randomizer & derandomizer

D-flip flop

```
LIBRARY ieee;
USE ieee.std_logic_1164.all;
USE ieee.std_logic_arith.all;

ENTITY d_ff IS
-- Declarations
      port(clk,rst,d,en: in std_logic;
               q: out std_logic);
END d_ff ;

-- hds interface_end
ARCHITECTURE rtl OF d_ff IS
BEGIN
     process(clk,rst,en)
     begin
       if(rst='1')then q<='0';
       elsif(rising_edge(clk))then
          q<=d;
          if(en='0')then q<='0';
          end if;
       end if;
    end process;
END rtl;
```

X-or

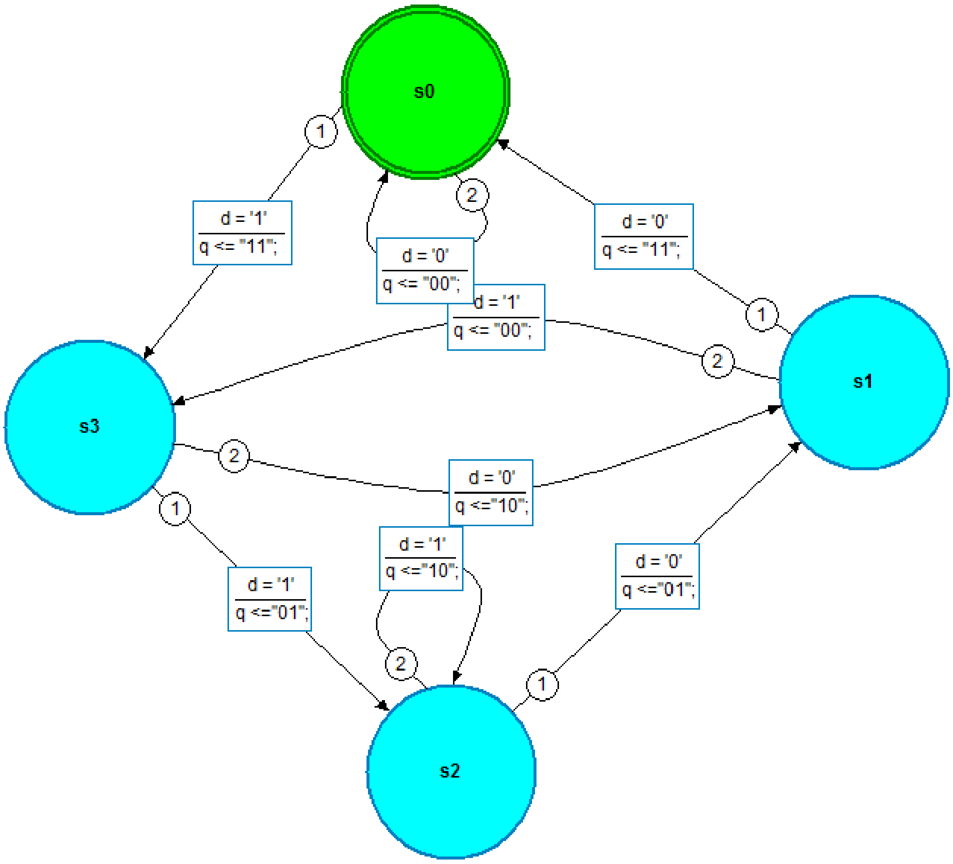
```
LIBRARY ieee;
USE ieee.std_logic_1164.all;
USE ieee.std_logic_arith.all;


ENTITY xor_gatte IS
-- Declarations
        port(a,b: in std_logic;
               c: out std_logic);
END xor_gatte ;

-- hds interface_end
ARCHITECTURE rtl OF xor_gatte IS
BEGIN
 c<= a xor b;
END rtl;
```

Reed Solomon

```
-- Declarations
            port (clk, rst, din,en: in std_logic;
          crc_sum: out std_logic_vector(7 downto 0));

END Reed_Solomon ;

-- hds interface_end
ARCHITECTURE rtl OF Reed_Solomon IS
     signal X: std_logic_vector(7 downto 0);

begin
     process(rst, clk)
     begin
        if  rst = '1' then

            X(7)   <= '1';
            X(6)   <= '1';
            X(5)   <= '1';
            X(4)   <= '1';
            X(3)   <= '1';
            X(2)   <= '1';
            X(1)   <= '1';
            X(0)   <= '1';

            elsif rising_edge(clk) then
              if en = '1' then
                  X(0)   <= Din  xor X(7);
                  X(1)   <= X(0);
                  X(2)   <= X(1);
                  X(3)   <= X(2) xor Din xor X(7);
                  X(4)   <= X(3) xor Din xor X(7);
                  X(5)   <= X(4) xor (din xor X(7));
                  X(6)   <= X(5);
               X(7)   <= X(6);

              end if;
          end if;
     end process;
     crc_sum <= X;
END rtl;
```

Appendix

Convolution coding & decoding



Inter leaving

```
ENTITY interleaving_code IS
-- Declarations
   port(x:in std_logic_vector(27 downto 0);
        y:out std_logic_vector(27 downto 0));
END interleaving_code ;

-- hds interface_end
ARCHITECTURE rtl OF interleaving_code IS
BEGIN
y<=x(27)&x(20)&x(13)&x(6)&
   x(26)&x(19)&x(12)&x(5)&
   x(25)&x(18)&x(11)&x(4)&
   x(24)&x(17)&x(10)&x(3)&
   x(23)&x(16)&x(9)&x(2)&
   x(22)&x(15)&x(8)&x(1)&
   x(21)&x(14)&x(7)&x(0);

END rtl;
```

De- inter leaving

```
ENTITY deinterleaving_code IS
-- Declarations
   port(x:in std_logic_vector(27 downto 0);
       y:out std_logic_vector(27 downto 0));
END deinterleaving_code ;

-- hds interface_end
ARCHITECTURE rtl OF deinterleaving_code IS
BEGIN
y<=x(27)&x(23)&x(19)&x(15)&x(11)&x(7)&x(3)&
   x(26)&x(22)&x(18)&x(14)&x(10)&x(6)&x(2)&
   x(25)&x(21)&x(17)&x(13)&x(9)&x(5)&x(1)&
   x(24)&x(20)&x(16)&x(12)&x(8)&x(4)&x(0);

END rtl;
```

Mapping

```
ARCHITECTURE rtl OF mapper IS
signal i sig: std logic vector(8 downto 0);
    signal count1:std_logic_vector(2 downto 0):=(others=>'1');

    begin
        process( clk,clr)
            variable b var:std logic;
            variable b_16 :std_logic_vector(1 downto 0);
            variable b_64,count:std_logic_vector(2 downto 0):="000";
            variable b: std_logic_vector(2 downto 0):
            begin
              if (clr='1')then
                    I<=(others=>'0');
                    Q<=(others=>'0');
                    count:=(others=>'0');

              elsif en='1' then
                    if(clk'event and  clk='1')then
                   count1<=count;

                 b_var:=serial_in;
                 case mod_sel is
                     when "00" => --BPSK
                         Q<="000000000";
                         if(b_var='0') then
                             I<="110000000";      --(-1)
                         else
                            I<="010000000";       --(1)
                        end if;
                        when "01" => --QPSK

                            case count is
                                when "000" =>
                                  if(b_var='0')then
                                    i_sig<="110100110";    --(-1/sqrt(2))
                                  else
```

Appendix

De-mapping

```
ARCHITECTURE rtl OF demapper IS
signal count: std_logic_vector(2 downto 0):=(others=>'0');
      signal BD1,BD2,BD3,BD4,BD5,BD6,sub1,sub2,sub3,sub4:std_logic_vector(8 downto 0):=(others=>'0');
        begin
        process( clk,clr)
          begin
              if (clr='1')then
                    count<=(others=>'0');
                    sub1<=(others=>'0');
                    sub2<=(others=>'0');
                    sub3<=(others=>'0');
                    sub4<=(others=>'0');
                    BD1<=(others=>'0');
                    BD2<=(others=>'0');
                    BD3<=(others=>'0');
                    BD4<=(others=>'0');
                    BD5<=(others=>'0');
                    BD6<=(others=>'0');

                        elsif (en='1') then
                            if(clk'event and  clk='1')then
                    case mod_sel is
                        when "00" => --BPSK
                           if(I(8)='0')then
                              serial_out<='1';
                           else
                              serial_out<='0';
                           end if;
                        when "01" => --QPSK
                            count <=count+'1';
                            case count is
                                when "000"=>  -- at this clk we have I,Q
                                  if (I(8)='0') then    --to get b0
                                      serial_out<= '1';
                                  else
                                      serial_out<='0';
                                  end if;
                                when "001"=>
```

Cyclic

```
ENTITY add_cyc_pre IS
-- Declarations
port( A: in std_logic_vector (223 downto 0);
      B: out std_logic_vector (251 downto 0));
END add_cyc_pre ;

-- hds interface_end
ARCHITECTURE rtl OF add_cyc_pre IS
BEGIN
B<= (A(27 downto 0)&A(223 downto 0));
END rtl;
```

Reference

1 Jeffrey G. Andrews , Arunabha Ghosh and Rias Muhamed. "Fundamentals of WiMAX (Understanding Broadband Wireless Networking)". Prentice Hall Communications Engineering and Emerging Technologies Series. Copyright © 2007 Pearson Education, Inc.

2 Ramjee Prasad. "OFDM for Wireless Communications Systems". Artech House universal personal communications series). Copyright © 2004.

3 Hui Liu and Guoqing Li. "OFDM-Based Broadband Wireless Networks (Design and Optimization)". A JOHN WILEY & SONS, MC.Publication. Copyright © 2004.

4 Ahmed R. S. Bahai and Burton R. Saltzberg. "Multi-Carrier Digital Communications (Theory and Applications of OFDM)". Kluwer Academic/ Plenum Publishers, NewYork, 1999 .

5 IEEE 802.16 Working Group. "Technical Overview of Wireless MAN Air Interface for Broadband Wireless Access". IEEE , 2003.

6 IEEE 802.16 Working Group."Channel Models for Fixed Wireless Applications". IEEE , June 2003.

7 WiMAX Forum. "Mobile WiMAX – Part I: A Technical Overview and Performance Evaluation", WiMAX Forum, August 2006.

8 Coring Inc."Broadband Techology Overview". June 2005.

9 Eugene Crozier and Allan Klein. "WiMAX Technology (LOS and NLOS environments) White Paper". SR Telecom, August 2004.

10 Yu,Chia-Hao. "Orthogonal Frequency Division Multiplexing". February 2006.

11 Domenic FARNESE. "Techniques for Peak Power Reduction in OFDM Systems". CHALMERS UNIVERSITY OF TECHNOLOGY, 1997-1998.

13 Amalia Roca." Implementation of a WiMAX simulator in simulink".Vienna, February 2007.